Heterogeneous Wireless Networks QoE Framework

HETEROGENEOUS WIRELESS PUBLIC NETWORKS IN A 5G WORLD

Xavier Jover Segura

March 2015

A thesis submitted for the Degree of Engineering Doctor of the University College London

Department of Electronic and Electrical Engineering

University College London (UCL)

Torrington Place, London WC1E 7JE

Declaration

I, Xavier Jover Segura confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Abstract

With the appearance of small cells and the move of mobile networks towards an all-IP 4G network, the convergence of these with Wi-Fi becomes a possibility which at the same time opens the path to achieve what will become 5G connectivity. This thesis describes the evolution of the different mainstream wireless technologies deployed around the world and how they can interact, and provides tools to use this convergence to achieve the foreseen requirements expected in a 5G environment and the ideal user experience.

Several topics were identified as needing attention: handover between heterogeneous networks, security of large numbers of small cells connected via a variety of backhaul technologies to the core networks, edge content distribution to improve latency, improvement of the service provided in challenging radio environments and interference between licensed and unlicensed spectrum. Within these topics a contribution was made to improve the current status by analysing the unaddressed issues and coming up with potential improvements that were tested in trials or lab environment.

The main contributions from the study have been:

1. A patent in the wireless security domain that reuses the fact that overlapping coverage is and will be available and protects against man in the middle attacks (Section 5.3).
2. A patent in the content distribution domain that manages to reduce the cost to deliver content within a mobile network by looking for the shortest path to the requested content (Section 6.3).
3. Improvements and interoperability test of 802.21 standard which improves the seamlessness of handovers (Section 4.2).
4. 2 infill trials which focus on how to improve the user experience in those challenging conditions (Sections 7.2 and 7.3).
5. An interference study with Wi-Fi 2.4GHz for the newly allocated spectrum for 4G (Section 8.2).

This thesis demonstrates some of the improvements required in current wireless networks to evolve towards 5G and achieve the coverage, service, user experience, latency and security requirements expected from the next generation mobile technology.

Acknowledgements

I wish to express my sincere gratitude to my supervisor, Dr. Kai Kit Wong for supporting and encouraging me during these last few years to undertake the EngD adventure in Mobile Communications at University College London and also for not allowing me to give up after nearly dropping out three times.

I would like thank British Telecom, my employer, and all the managers I have had during these past few years (F. Jover Aparicio, Dr. D. Wisely, Dr. F. De Carvalho, M. Cuevas, A. Fidler, T. Brown and Dr. W. Chooi) for allowing me to complete the EngD, all the associated modules, and provide advice and guidance.

I want to thank my friends and colleagues for their sincere support and words of encouragement when I thought I was not up to the task. Thanks Santosh and Deveril.

I also want to Samantha Muncaster for all the support she has provided over these years and the final push to complete this Thesis. Without her I wouldn't have been able to complete it.

Finally, my deepest appreciation goes to my kids, Nico, Marcos and Neo, for their patience and the many hours I have stolen from them to complete this Thesis.

Abbreviations

2G	2nd Generation of Mobile Networks
3G	3rd Generation of Mobile Networks
3GPP	3rd Generation Partnership Project
4G	4th Generation of Mobile Networks
5G	5th Generation of Mobile Networks
AAA	Authentication Authorization and Accounting
ACS	Adjacent Channel Selectivity
AH	Authentication Header
AKA	Authentication and Key Agreement
ANDSF	Access Network Discovery and Selection Function
ANQP	Access Network Query Protocol
AP	Access Point
APN	Access Point Name
AuC	Authentication Centre
BBC	British Broadcasting Corporation
BET	Broadband Enabling Technology
BSC	Base Station Controller
BSS	Base Station System
BT	British Telecom
BTOZ	BT OpenZone aka BT Wi-fi
BTS	Base Transceiver Station
CDN	Content Delivery Networks
CEPT	European Conference of Postal and Telecommunications Administrations
CGRF	Content-based Gateway Re-selection Function
CL	Content Locator
CPE	Customer Premise Equipment
CPU	Central Processing Unit
CSFB	Circuit Switched Fall-Back
DA2GC	Direct Air to Ground Communications
DPI	Deep Packet Inspection
DL	Downlink
DNS	Domain Name Server
DoS	Denial of Service
DSA	Digital Signature Algorithm
DTTV	Digital Terrestrial Television
E2E	End-to-End
EAP	Extensible Authentication Protocol
ECC	Electronic Communications Committee
EDGE	Enhanced Data for GSM Evolution
EE	Everything Everywhere
EIR	Equipment Identity Register
EIRP	Equivalent Isotropically Radiated Power
eNB	Enhanced Node B

EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standard Institute
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FDD	Frequency Division Duplex
FMCA	Fix Mobile Convergence Alliance
GAS	Generic Advertisement Service
GDB	General Dynamics Broadband
GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
GPRS	Generic Packet Radio Service
GSA	Global mobile Suppliers Association
GSM	Global System for Mobile Communications
GTP	GPRS Tunnelling Protocol
GW	Gateway
HD	High Definition
HLR	Home Location Register
HO	Handover
HSCSD	High Speed Circuit Switched Data
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IARP	Inter-APN Routing Policy
IDCM	InterDigital Connection Manager
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IMS	Internet Multimedia Subsystem
IMT	International Mobile Telecommunications
IOT	Interoperability Testing
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IS	Information Server
ISG	Intelligent Services Gateway
iSIP	Intelligent SIP
ISM	Industry, Scientific, Medical
ISMP	Inter System Mobility Policies
ISP	Internet Service Provider
ISRP	Inter System Routing Policies
KPI	Key Performance Indicator
KT	Korea Telecom
LCS	London Communications Symposium

LTE	Long Term Evolution
LTE-A	LTE Advance
M2M	Machine to Machine communications
MAC	Media Access Control
MAPCON	Multi Access PDN Connectivity
MB	Megabyte
MEAS	Managed Ethernet Access Service
MICS	Media Independent Command Service
MIES	Media Independent Event Service
MIH	Media Independent Handover
MIIS	Media Independent Information Service
MIMO	Multiple Input Multiple Output
MLS	Multilayer Switching
MME	Mobility Management Entity
MNO	Mobile Network Operator
MOCN	Multi Operator Core Network
MOS	Mean Opinion Score, where 1 is lowest perceived audio quality, and 5 is the highest percei quality measurement
MSC	Mobile-services Switching Centre
MSS	Mobile Satellite Service
MWC	Mobile World Congress
NA	Not Applicable
NB	Node B
NFC	Near Field Communications
NLS	Network Location Server
NOC	Network Operator Centre
NSN	Nokia Siemens Networks
NSWO	Non-Seamless WLAN Offload
NW	Network
OEM	Original Equipment Manufacturer
OPIIS	Operator Policies for IP Interface Selection (TR23.853)
OTT	Over The Top
PCRF	Policy and Charging Resource Function
PGW	PDN (Packet Data Network) Gateway
PL	Packet Loss
PoA	Points of Attachment
PoC	Proof of Concept
PoP	Point of Presence
PoS	Point of Service
PTP	Precision Time Protocol
QCI	QoS Class Identifiers
QoE	Quality of Experience
QoS	Quality of Service
R&T	Research and Technology

RAN	Radio Access Network
RDF	Resource Description Framework
RF	Radio Frequency
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Receive Signal Strength Indication
RTCP	Real-Time Control Protocol
RTSP	Real Time Streaming Protocol
SA	Security Association
SaMOG	S2a Mobility over GTP
SD	Standard Definition
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SIM	Subscriber Identity Module
SINR	Signal to Interference plus Noise Ratio
SIP	Session Initiation Protocol
SoR	Statement of Requirements
SRVCC	Single Radio Voice Call Continuity
SSID	Service Set Identifier
TB	Terabyte
TC	Test Case
TCP	Transport Control Protocol
TDD	Time Division Duplex
TLV	Type Length Value
TTLS	Tunnelled Transport Layer Security
TWAG	Trusted Wireless Access Gateway
TX	Transmission
UDP	User Datagram Protocol
UE	User Equipment
UKB	UK Broadband
UL	Uplink
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
UWB	Ultra WideBand
UX	User Experience
VLC	Visible Light Communications
VLR	Visitor Location Register
VPN	Virtual Private Network
VVOIP	Voice and Video over IP
WAP	Wireless Application protocol
WCC	Wholesale Content Connect
WCDMA	Wideband Code Division Multiple Access

WLCP	Wireless LAN Control Protocol

Table of Contents

List of Figures

List of Tables

Chapter 1: Summary

1.1.Contributions

After an initial study of the past, current and future of wireless technologies in Chapter 2 it was decided that in order to move into what was starting to be considered as 5G or future of wireless networks, there were a few key areas that needed addressing. This thesis' contributions are mostly centred on these 5 key areas which according to the author are in need of improvement (amongst others).

The following list provides a high-level overview of the various contributions in the key identified areas:

- HANDOVER Section 4.2: Early implementation of IEEE (Institute of Electrical and Electronics Engineers) 802.21 MIIS (Media Independent Information Service) with integration with a SIP (Session Initiation Protocol) VVOIP (Video and Voice over IP) Windows client (also developed by the author called iSIP, intelligent SIP) to demonstrate seamless handover between Wi-Fi, WiMAX and 3G. The handover was of the type make-before-break and no packets were lost, which meant there was no compromise to UX during HO and proved the validity of 802.21 as seamless handover enabler. The demonstration was done in collaboration with NSN (Nokia Siemens Networks) and Intel, and it was demonstrated in the MWC (Mobile World Congress); results were directly fed into the standard [1]. The same service was integrated with a SIP mobile client and demonstrated also in MWC in collaboration with InterDigital.
    - Participated with IEEE 802.21 in FMCA (Fix Mobile Convergence Alliance) organized plugfest for interoperability testing with the BT (British Telecom) MIIS, output conclusions were feed into the standard to clarify future implementations, as incompatibility due to the different supported payloads was found to be an issue. A solution was tested using an MIH Proxy developed by the author, which allowed to complete the tests where the incompatibility was an issue.
    - ISIP client 100% developed by the author. Versions for Windows and windows Mobile, code available in third party website [2].
- INTERFERENCE Section 8.1: Study and report of Wi-Fi/LTE FDD (Frequency Division Duplex) interference in the 2.6 GHz band (LTE band 7), which showed that:
    - It was possible to cause substantial reductions (>50%) to Wi-Fi throughput at LTE power levels above 15 dBm (31 mW) and where the LTE transmitter was within 3 m of the Wi-Fi stations or access points.

    - When the LTE simulator was in very close proximity <1 m to the Wi-Fi device or access point then Wi-Fi data throughput could be reduced to zero across the entire 2.4 GHz band.
    - Due to the nature of the frequency band allocation (in the UK), interference would be most significant from Vodafone mobile subscribers transmitting to LTE base stations at higher powers.
    - Additional hardware filtering, more intelligent Wi-Fi channel selection [3], Cognitive radio techniques [4] or rate control algorithms may be required [5].
- INFILL Section 7.1: Managed and delivered a report on the performance of the world first LTE network in MOCN (Multi Operator Core Network) in collaboration between BT and EE (Everything Everywhere) in advance of their deployment of LTE. At the same time this was the world first trial delivering broadband over LTE in rural areas. The user perceived QoE was better than expected and by trialist request the trial was extended until BT was ready to deploy fibre connectivity to the area (+6 months). EE gained a lot of insights from the trial and currently are offering broadband over LTE in Cumbria as a commercial service [6]. Some of the outputs used by EE include:
    - Management of QoE between mobile and mobile-fix subscribers via HSS (Home Subscriber Server) and radio network configuration.
    - Techniques to avoid congestion by data hungry multi-device households via PCRF (Policy and Charging Resource Function) rules, see Section 7.2.1.
    - Radio measurements to estimate new fix subscriber potential speeds before allowing them into the service.
    - Expected data usage over the course of the day on a rural community.
- PATENT 1: SECURITY, see Section 5.3 for details [7] , patent to reuse 802.21 MIH Information Server or ANDSF with some enhancements to allow non-802.1x compliant devices and access points to securely authenticate via the previously authenticated mobile network and hence eliminating the possibility of connecting to Rogue access points.
- PATENT 2: CONTENT DISTRIBUTION, see Section 6.3 for details [8], patent filed to deliver enhanced content distribution on 4G (4th Generation of Mobile Networks) networks by taking into account both the user location and the content location to calculate the most beneficial path for the mobile operator.

1.1.1. Publications

Apart from the above two patents, the following papers and posters were published as part of the results from this thesis:

- LCS (*London Communications Symposium*): X. Jover Segura, "QoE in Femtocells," in *London Communications Symposium*, London, 2010 [9].

- Barlow posters: 2011 - QoE for femtocells; 2013 - Mobile Network Gateway Reselection.

Mildner posters: 2010 - Future Backhaul Access Bottleneck Study.

1.2. Definitions

Definitions of terms widely used in this thesis:

Throughput: the amount of data transmitted over a telecom network successfully from one node to another in a given time period, typically measured in bits per second (bps), megabits per second (Mbps) or gigabits per second (Gbps).

Latency: the total time it takes a data packet to travel in between two specific nodes.

Coverage: of a radio station is the geographic area where the station can communicate successfully.

Capacity: Highest possible reliable transmission rate that can be carried on a specific system or equipment

Bit Error Rate: In a transmission, the percentage of bits that have errors when compared to the total number of bits received.

Signal-to-noise ratio (SNR): Comparison of the level of a desired signal to the level of the background noise.

QoS: the overall performance as seen by the users of the network. To quantitatively measure quality of service, several related aspects of the network service are often considered, such as error rates, bit rate, throughput, transmission delay, availability and jitter.

QoE: To understand the Quality of Experience delivered to customers, operators cannot just monitor the network, the NOC (Network Operator Centre) might be fully functional and the subscribers might still perceive degraded service [10]. So a different way to understand the delivered service needs to be used that carefully balances the following amongst others:

- Signal quality received by the individual.
- Number of connections that simultaneously use the network in an area.
- Performance of a particular handset.
- Download bitrate.

These are difficult to monitor [11] [12] [13] and therefore easier to measure key parameters have been used over this thesis [14]: delay, received bitrate and jitter, which require to reach a certain threshold to allow the applications and services a particular user in a particular location would request.

Chapter 2: Introduction

The development of what has become the two most successful and popular wireless technologies, Wi-Fi and mobile networks, has been done without taking into account each other, this is true especially in their beginnings as they were originally designed for different purposes [15] [16], some for voice some for data, some mobile and some nomadic, but at the end, they have all evolved to carry data (IP, Internet Protocol) [17] and are used in the same devices and run the same services. As a consequence, the need to cohabitate and collaborate becomes key and even crucial to deliver the requested user experience, which has been growing as new improvements and features have appeared, increasing expectations [18].

Traditionally different wireless technologies had little interaction and did not acknowledge the existence of each other [17]. This was partly because:

- different specialized devices were used to interact with each of the wireless technologies
- the types of data consumed were different [19]
- as Wi-Fi used license free spectrum, lacked macro coverage and used bigger devices, it was considered to be a nomadic opportunistic wireless technology [20].

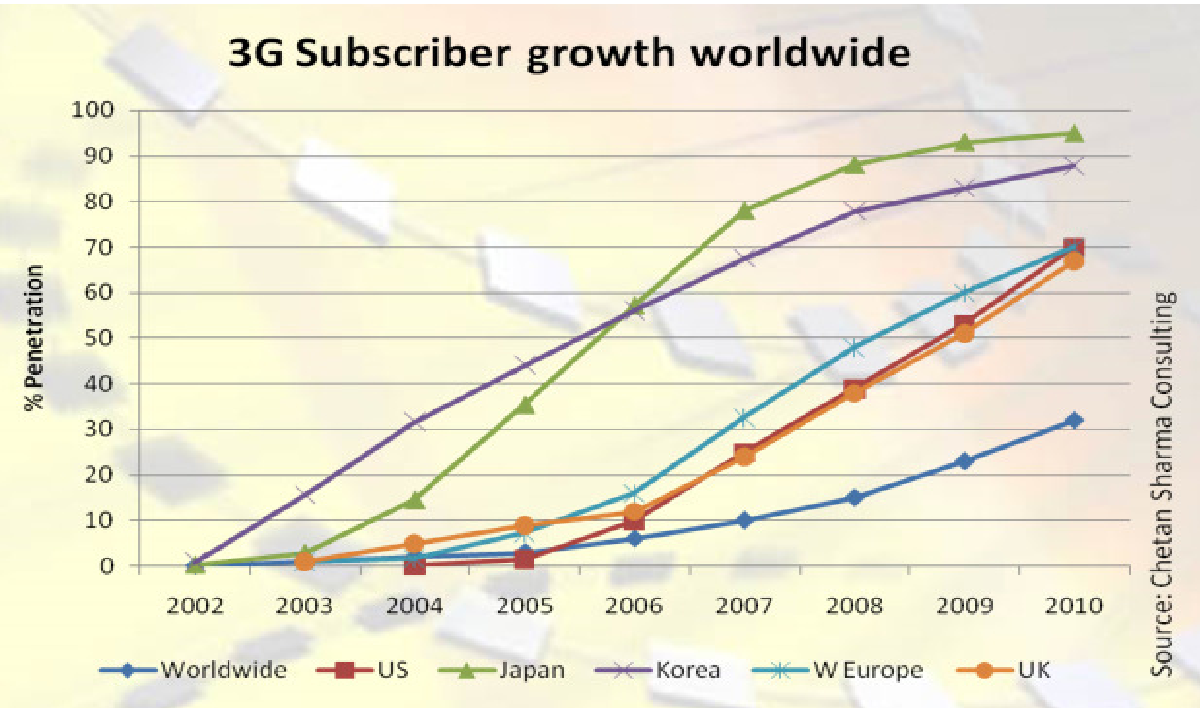


Figure 1 - 3G subscriber growth worldwide (Source: Chetan Sharma Consulting).

Wi-Fi slowly started to become more popular and more devices started to be capable of connecting to it, initially laptops and later a few mobile phones (1999 to 2003) [21]. At the same time, mobile networks started carrying a small amount of data, WAP (Wireless

Application protocol) was introduced in 1999, but it was not until 2003 with the introduction of 3G (3rd Generation of Mobile networks), that a decent amount of bandwidth was supported and data consumption in mobile devices started to grow, on average by 400% a year between 2004 and 2010 [22], creating the new expectation that a good mobile network had to be able to provide good data rates to subscribers. From 2003 onwards, we started having two networks capable of data delivery in the same device. The truth is that at this point Wi-Fi coverage was very uneven, the mobile network speed achievable was still not very high and, what is even more important, the mobile devices (hardware, OS, and software applications) were not user friendly enough to consume a great amount of data so, as a result, the majority of subscribers were not aware of the network capability [23].

All this changed again with the appearance of smartphones around 2007. At that moment the amount of data consumed via mobile devices globally exploded [24](Figure 1), and has continued to grow exponentially since, creating a real problem to mobile operators that could not deliver the expected amount of bandwidth at the low cost it was requested [25] (Figure 2).

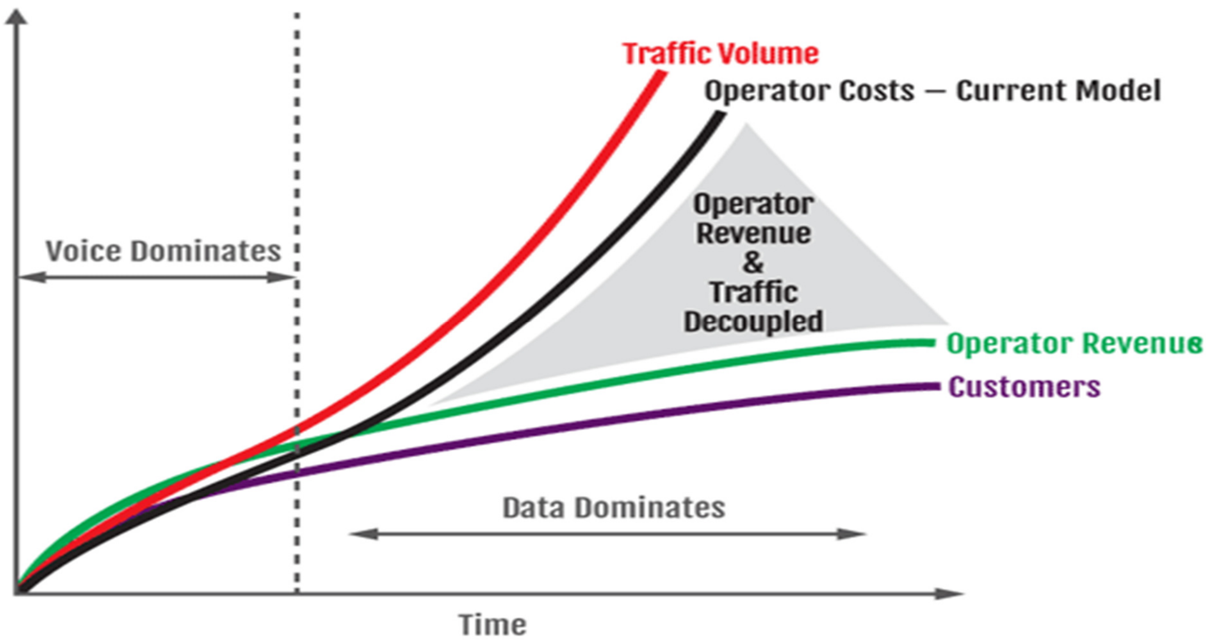


Figure 2 - Discrepancies between traffic growth and revenue growth (Source: Accenture).

In Figure 2, it is clearly seen the dilemma created by the new “needs” of the subscribers, more and more data at a lower and lower cost (even zero cost [25]).

In Figure 3, we can see the predictions for the mobile world data traffic for the coming years. Cisco has been predicting the mobile data growth since 2007 for the following 5 years and their predictions are usually quite accurate.

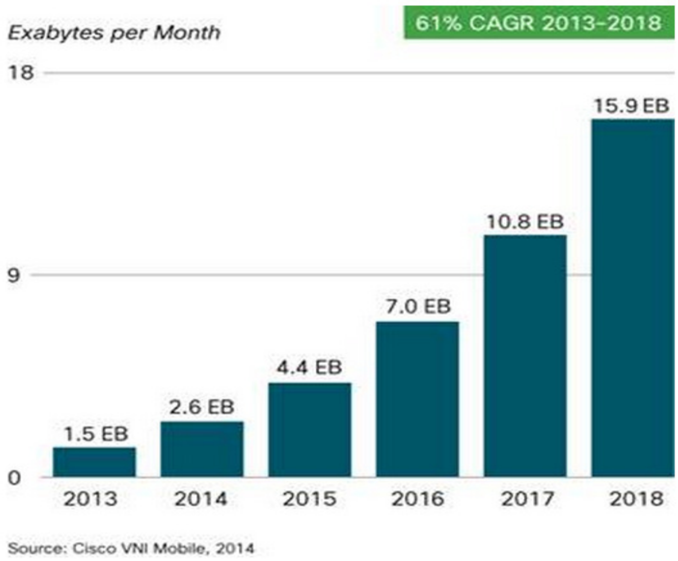


Figure 3 - Cisco predictions of mobile data traffic growth (Source: Cisco).

The hunger for data from mobile devices could not, and cannot, be met by a single technology [26], but initially no effort was made to associate different wireless technologies to deliver the required results. The mobile operators struggled to offer the amount of data requested at the cost expected. This precipitated the move from a voice centric network circuit based to a data centric packet based network, LTE (Long Term Evolution), which has allowed the operators to deliver data at a much lower cost per MB (Megabyte), but, according to predictions [27] [28], this alone won't be enough, small cells and especially Wi-Fi, would be needed to meet the future demands.

The introduction and integration of Wi-Fi into the mobile world needs to be done in a way that improves the experience of the mobile subscribers without damaging or disrupting the seamlessness expected from a mobile service.

2.1.Motivation

The trend to consume more data is only going to increase with technologies like Cloud (cloud services, cloud storage and even cloud computing), 4K video streaming (which requires a minimum 15Mbps stable connection or a maximum of 50 Mbps [29]) and virtual reality.

Subscribers are not interested in which technology is used to deliver their service as long as the experience is good enough or seamless to them [30] and at the right cost.

The aim of this thesis is to analyse the best way in which heterogeneous wireless technologies can deliver the required data capacity and the adequate QoE (Quality of Experience) while moving towards what is considered the ideal 5G (5th Generation of Mobile Networks) environment. To achieve this, several different key study areas from within the wireless network technology subject need to be coordinated:

- Data needs to be protected E2E (End-to-end) without any possibility of it being intercepted; the level of security shouldn't be different depending on which technology or method it is used to deliver the data.
- The user should not need to be aware of handovers between different technologies, or which technology is in use (unless they want to).
- Data needs to be segregated and each segregated data element needs to be sent over the most adequate connection/technology in order to use and organize the resources in the most sustainable way.
- Access should be available everywhere regardless of where in the country you are. Some technologies will be best applied to urban, semi-urban, or rural scenarios.
- Operators must interact with the device ecosystem via standardization to provide the 5G user experience and seamlessness.
- Latency needs to be lower, therefore apart from faster backhaul technologies, the content needs to be brought closer to the consumer to deliver these low latencies and user experience expected.

UX (User Experience) and capacity achievable will be the differentiator between the various providers as the price of data goes down [31], in that case, technologies/standards that try to break differentiation between mobile networks and Wi-Fi networks, like 802.21 (aka MIH, Media Independent Handover) and 3GPP (3rd Generation Partnership Project) ANDSF (Access Network Discovery and Selection Function), will become most useful to operators.

Mobile operators will have very different amounts of mobile spectrum (which they can combine using the latest technologies like LTE-A, LTE Advance), and different ways to access Wi-Fi networks, therefore the different techniques to manage them together with the device behaviour will be the key to maintain control on the QoE and the cost per MB.

In this case, the capability of tweaking the device behaviour to better use the mobile operator resources is very important. For example, currently iOS uses a carrier file which is automatically downloaded on the first boot for each specific operator with whom Apple has a direct relationship with, this carrier file contains up to 300 parameters which are tailored to each of Apple's mobile partners [32]. There are other players in the industry, like Google, Samsung and HTC, which are considering implementing a similar solution to customize their devices to the networks they are in. This file, hence, becomes another possible candidate to transmit the operators rules on how to make use of the heterogeneous environment the devices will encounter.

Chapter 3: Overview of Past, Current and Future Wireless Environment

The two most common wireless access technologies currently available to consumers are Wi-Fi and 3GPP mobile networks. Both are currently focussed on data connectivity which is what will help their future integration, but they had very different beginnings, see Figure 4.

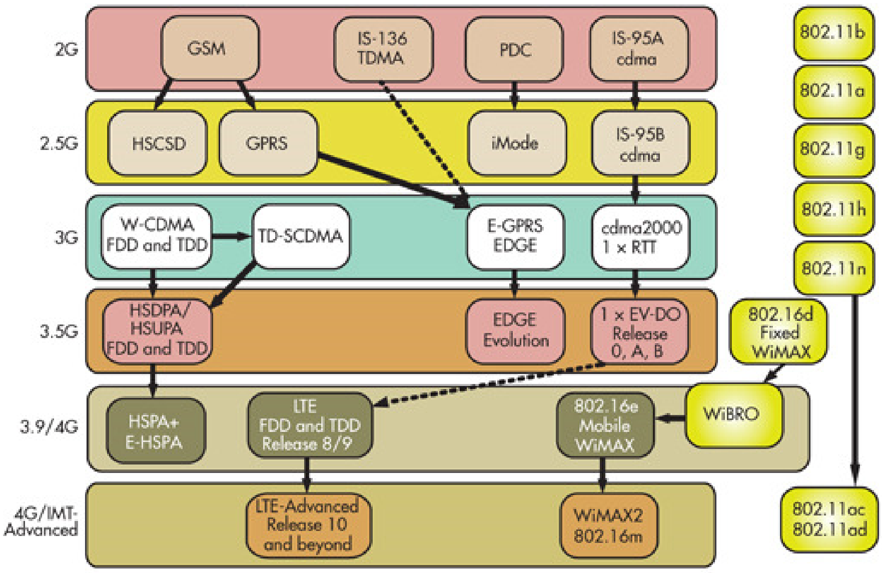


Figure 4 - Mobile networks and Wi-Fi evolution (Source: electronicdesign.com [33]).

3.1. 3GPP Mobile Network Evolution

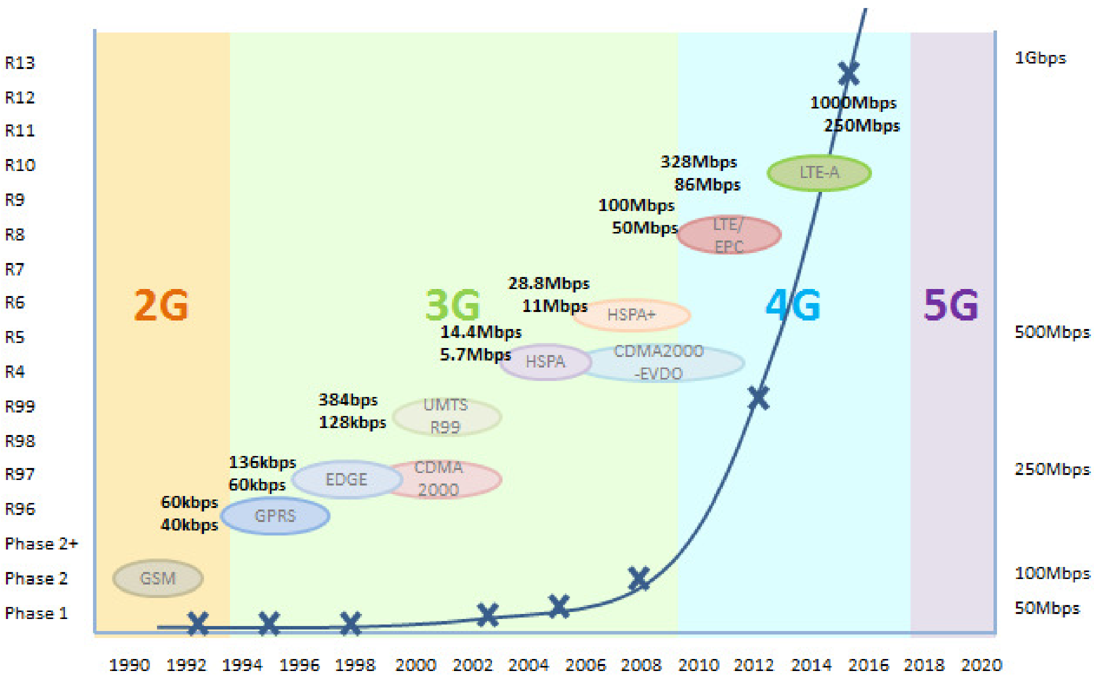


Figure 5 - 3GPP standard release history vs achievable speeds (Data Source: Wray Castle Limited).

Traditional 3GPP mobile networks were originally designed for voice, and consequently they were built mimicking the PSTN network of those days, therefore based on circuit-switched networks. In the beginning of the 1990s GSM (Global System for Mobile Communications) networks (2G, 2nd Generation of Mobile Networks) started to deploy around the globe [34]. The new system used digital modulation for the first time, which improved the voice quality but the amount of data that was capable of sending was very restricted (9.6 kbps up to 19 kbps [34]), see Figure 5. The initial aim of the operators was to improve the coverage and the transmission quality and data was just added as an after though. The data services available at that time were WAP, HSCSD (High Speed Circuit Switched Data) and MLS (Multilayer Switching).

In the second half of the 1990s, GPRS (Generic Packet Radio Service) was introduced as a way to deliver packet switched services in a circuit switched GSM network with a theoretical transfer speed of maximum 136 kbps (90 kbps in practice for downlink and 40 kbps in the uplink) [35]. A little bit later (1998), EDGE (Enhanced Data for GSM Evolution) was also introduced to increase the capacity with a theoretical transfer speed of maximum 384 kbps (250 kbps in practice), improving spectral efficiency and reducing latencies down to 100ms [36].

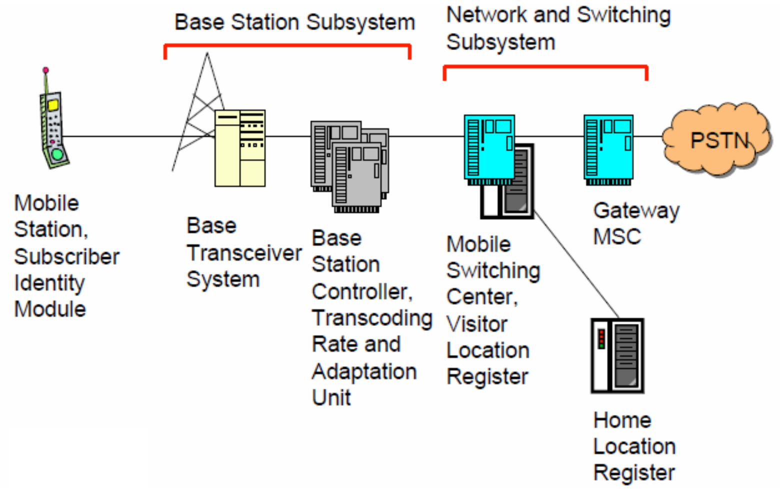


Figure 6 - GSM basic architecture (Source: Ali Usman [37]).

Above, in Figure 6, we can see the GSM architecture, in the MSC (Mobile-services Switching Centre) is where all the circuit switching for voice was done, it was really in essence a typical telephone exchange which supported mobile communications.

As the use of 2G phones was popularized it was clear that the demand for data services was growing [38]. For this reason, in the early 2000s 3G was introduced, first with GPRS and EDGE, which deployed architectural changes to deal with data in a real packet switch network, while voice was left on the circuit switched side [39]. Over 3G it was possible to watch streaming video but to do this it was required a non-congested network, in those circumstances 3G can deliver up to 2 Mbps. In worse conditions and with high speed moving subscribers the available bandwidth can drop to 145 kbps. In the second half on 2000s improvements to the radio layer (HSDPA, HSUPA, HSPA and HSPA+) meant that these speeds were improved up to 28.8 Mbps [40].

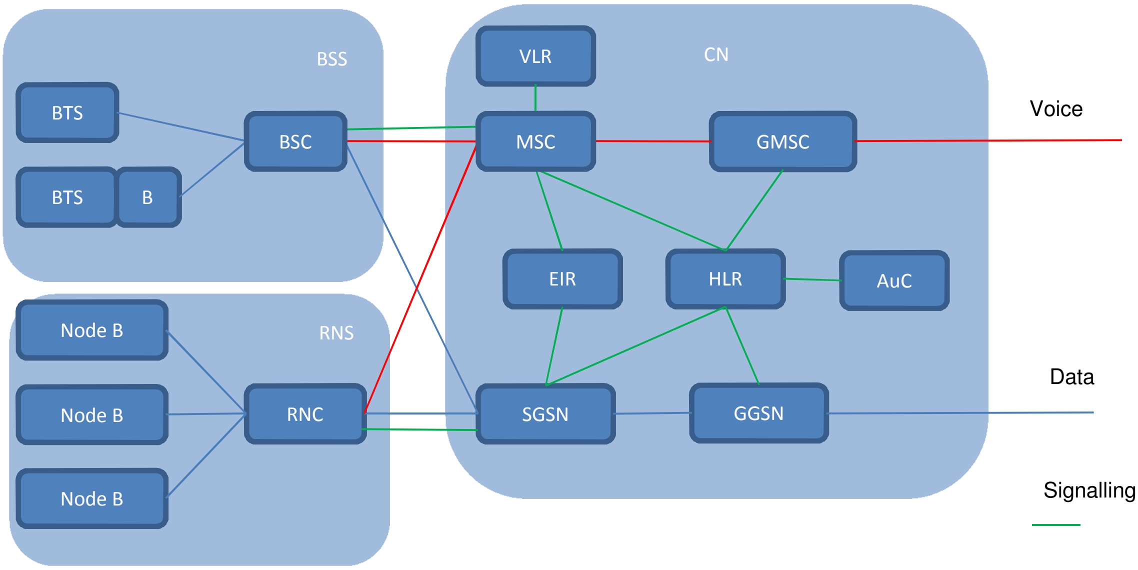


Figure 7 - Pre-LTE standard mobile network diagram (Data Source: 3GPP Standards).

Figure 7 Legend: AuC (Authentication Centre), BSC (Base Station Controller), BSS (Base Station System), BTS (Base Transceiver Station), EIR (Equipment Identity Register), GGSN (Gateway GPRS Support Node), SGSN (Serving GPRS Support Node), GMSC (Gateway MSC), RNC (Radio Network Controller), RNS (Radio Network Subsystem), VLR (Visited Location Register).

In the above Figure 7, we can see the structure of a 3G network that has to deal with both a circuit switched network for voice and a packet switched network for data.

3G could allow the usage of higher data rates which promoted the use of internet application services consumed from mobile network subscriber's devices. As more devices were able to use these applications and consume more data it was clear that the current network had not been designed for the amount of data requested by the end-users [41].

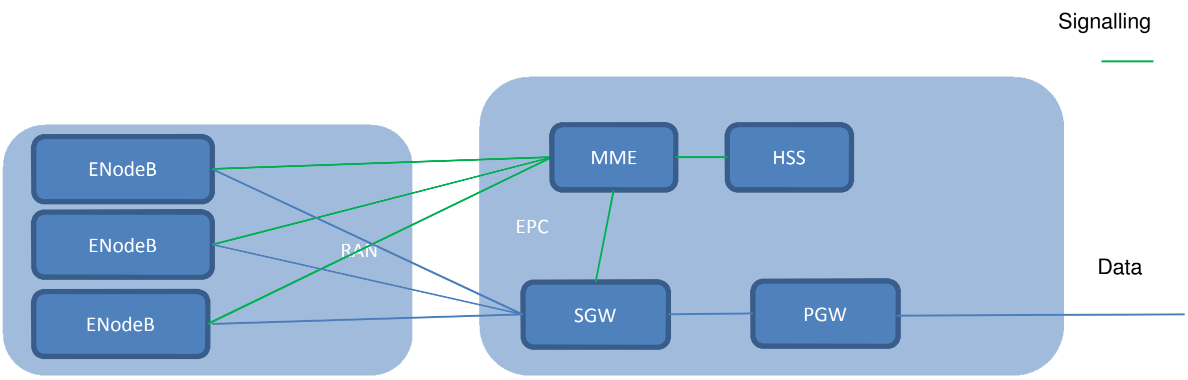


Figure 8 - Standard LTE only network diagram (Data Source: 3GPP Standards).

Figure 8 Legend: PGW (Packet Data Network Gateway), SGW (Serving Gateway).

Therefore at the beginning of 2010s, 4G (LTE) was designed to be an IP based network only [42]. Even voice was expected to be carried over IP in a packed switched way, reducing the core network complexity. LTE, in its first iterations, delivers up to 150Mbps [43] with later improvements that allowed delivering even higher data rates.

In Figure 8, we can see the much simpler design of an all-IP LTE-EPC (Evolved Packet Core) network, which will help with the increase of demand, see Figure 9, and the scalability of the mobile networks.

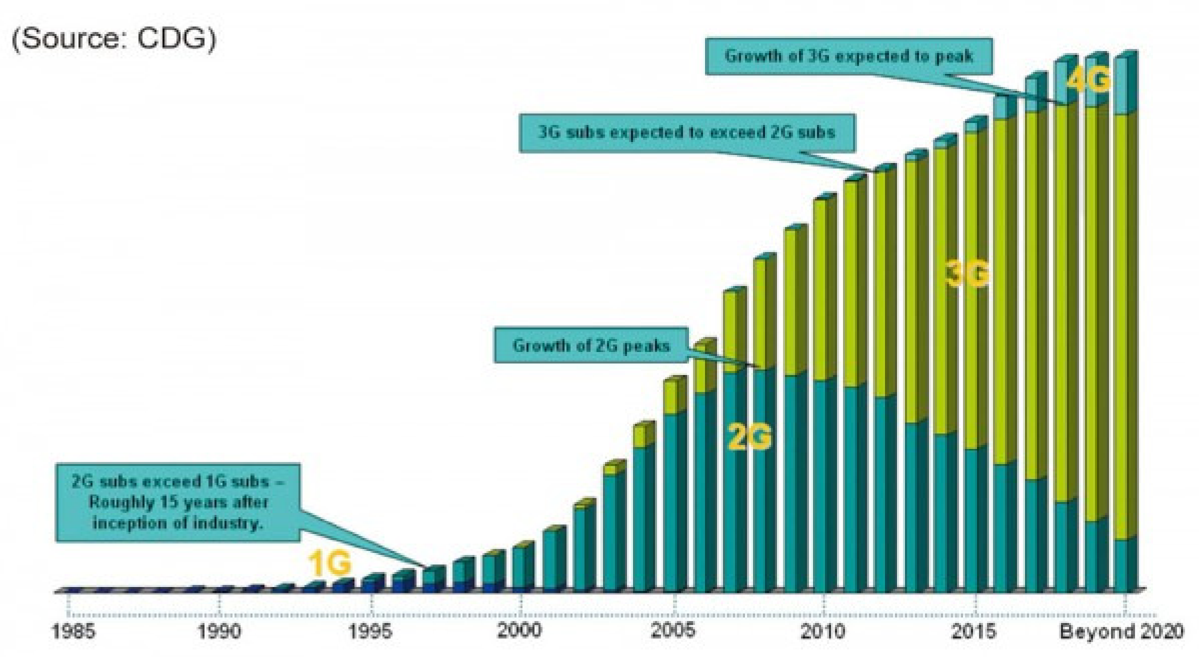


Figure 9 - Expected numbers of users globally for 2G, 3G and 4G (Source: CDG).

It is considered that now that the core network is all IP, the architecture and interfaces will not suffer major changes. Therefore any new evolution for the next 2 or 3 releases of the 3GPP standards will concentrate on the optimization of the radio access network and in decentralization of the core network to bring lower latencies [44]. For example, LTE Advance, aka LTE-A, will support carrier aggregation (aggregation of separate portions of spectrum, up to 5 of 20 MHz = 100 MHz), and higher MIMO (Multiple Input Multiple Output) orders both in the eNB (Enhanced Node B) and the devices [45].

Although there are still many different opinions on what 5G or the next evolution of mobile networks (around or after 2020) will be, what many experts agree is that 5G will [46]:

- Improve reliability.
- Increase bandwidth to a level of "perceived infinite capacity", estimated capacity gain of up to 1000x by 2020.

- Support the internet of things (wearables, probes, sensors).
- Provide lower latency.
- Deliver improved device autonomy.
- Achieve a more efficient use of the Spectrum (both licensed and un-licensed).

The key technologies to achieve these goals are:

- Indoor wireless access points for indoor usage to avoid in-out performance degradation. Technologies to use are:
  - Wi-Fi offload, an already widespread technology that needs to be more closely integrated into the mobile core network, as we will see in Section 3.4.1.
  - Femtocells, which provide coverage on the mobile operator spectrum in a very small area (see Section 3.4.3).
  - Ultra wide band (UWB) [47], which allow low energy short range high-bandwidth communications over at least 500MHz of spectrum and can share spectrum without interfering other systems.
  - Mm-wave communications (3–300 GHz) [48], with large spectrum but big propagation losses that make them ideal for indoor systems.
  - Visible Light Communications (VLC) (400–490 THz) [49], which uses visible light and can reach speeds of 500Mbps.
- Increase outdoor reliability, spectral efficiency, and energy efficiency using:
  - Distributed Antenna Systems (DAS) [50], a network of spatially separated antenna nodes connected to a common source via a transport medium that provides wireless service within a geographic area or structure, providing a much increased efficiency when compared to simple antennas.
  - Massive MIMO,
- Increase outdoor radio bandwidth using:
  - LTE-U
  - Cognitive Radio Networks.
- Reduce latency by:
  - Mobile core virtualization
  - Distributed mobile core

3.2. Wi-Fi Network Evolution

Although the idea of a wireless network using unlicensed spectrum started to have backers in the late 1980s [51] and governments allocated certain frequencies for it, it was not until 1999 with the ratification of IEEE of 802.11b that Wi-Fi really started to be deployed globally. 802.11b was theoretically capable of delivering up to 11Mbps in the 2.4GHz band (6Mbps in practice) [52], and was used mainly for small networks containing a few 10s of APs (Access Point) as a maximum. 802.11a was ratified in July 1999 [53] and delivered up to 54Mbps in the 5GHz band. In June 2003 802.11g was also accepted, delivering 54Mbps in the 2.4GHz spectrum [54].

In 2004, the first PDAs and phones started to have Wi-Fi integrated. This was the first contact between the 3GPP mobile networks and the IEEE wireless data standards in the same device.

In July 2009 802.11n is introduced [55]. This standard can work in 2.4GHz and 5GHz simultaneously, providing a combined speed of up to 900Mbps, see Figure 10.

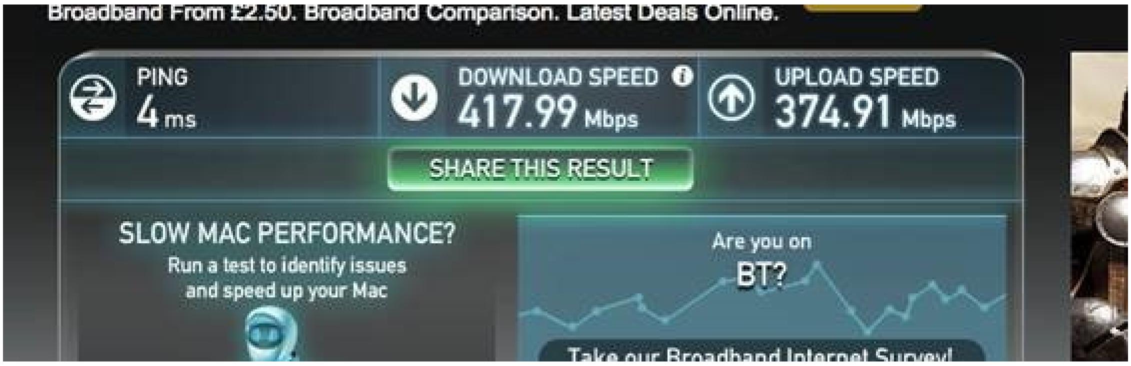


Figure 10 - MacBook connecting with 802.11n to a Cisco 3700 BT Wi-fi Access point with Etherflow backhaul.

From mid 2000s to the end of the decade the number of Wi-Fi hotspots increases to several million and the number of hotspots in the biggest Wi-Fi networks increases exponentially. BT OpenZone (aka BT Wi-fi) is one of the biggest Wi-Fi networks, it announced in 2012 7.5 million hotspots in the UK [56](currently over 8 million).

The high data rates and low price per MB made this technology interesting to mobile operators that were unable to deliver the required amount of capacity in their 3G networks. With 4G networks this issue was delayed, but as 4G networks become congested it is expected that Wi-Fi will also become more relevant [57]. The positive side is that this time LTE mobile networks have got already a defined architecture in the standard to accept Wi-Fi as part of the radio access network (3GPP TR 23.852 [58]).

3.3.What Made the Ecosystem Change?

As mentioned in the Section above, the appearance of PDAs and mobile phones with Wi-Fi which later became smartphones, made these finally the ideal devices to consume internet services on the move [59]. The iPhone, see Figure 11, with its big screen and touch interface, made finally attractive the idea of browsing the internet from a mobile device and many other mobile manufacturers copied the concept and produced their own version.

Figure 11 - First Apple iPhone (Source: Apple).

These devices were capable of processing and consuming more information, playing and streaming high definition video. Their popularity created pressure on the mobile networks to deliver more data to their subscribers in what is called in the industry as the "Data Tsunami" [60]. This request of more and more data is what initiated the move to 4G and the integration of Wi-Fi within mobile networks while searching for low cost delivery of data to end-user devices.

IPhone devices and the services they used, stopped being under the control of the mobile operator [61]. Devices have their own application stores and the services they provide, which took out another potential source of revenue from operators [62], are usually data-based OTT (Over the Top) without mobile operator interaction. From this point onwards operators lost control on how devices behaved within their networks, and the control went to the device manufacturers and wireless chip vendors, who decided how the device was going to behave when interacting with heterogeneous wireless scenarios. Because of the lack of standardization on device behaviour, and lack of control by operators, today there exists a great divergence on how the different devices perform in an heterogeneous wireless scenario and how many resources they require to maintain QoE (or even if they try to maintain any QoE instead of just supporting best effort).

Of course, it was not all due only to the appearance of the smartphone, but other simultaneous events/developments (see Figure 12) influenced as well as explained in [63]. The IoT (Internet of Things) [64], M2M (Machine to Machine communications) [65] [66] and control and sensing traffic has also been increasing but these are at the moment low bandwidth applications (requiring a constant connectivity and low latency) that currently aren't having a huge impact on the total mobile data traffic, although that is expected to change.

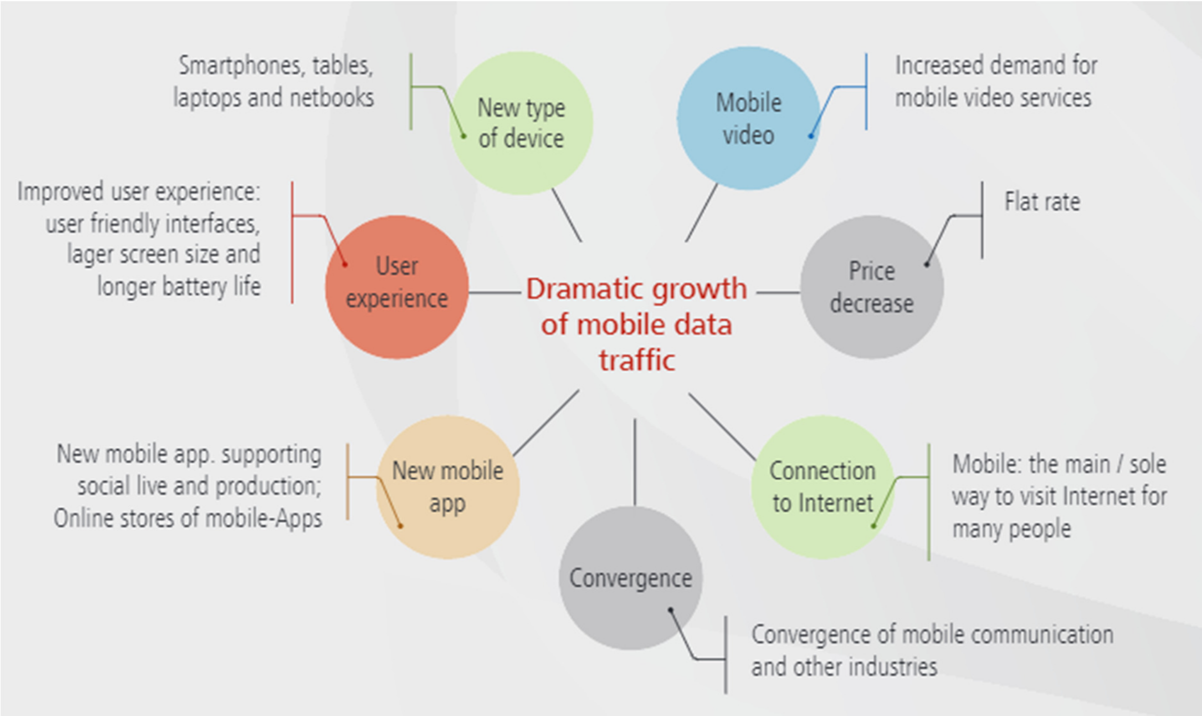


Figure 12 - Drivers of mobile date traffic increase (Source: Huawei [63]).

3.4.Current Status of Wireless Networks

There are a few different types of wireless access at the moment that can form part of the overall wireless network. These different types of access require the capability to interwork correctly in order to maximize user experience and throughput, while simultaneously decreasing the cost per MB for the mobile operator.

Next we will describe the different types of access that have been used to either, improve experience, improve throughput or decrease the cost per MB delivered from the mobile operator's point of view.

3.4.1. Wi-Fi Offload

Wi-Fi offload is called to the technique in which the mobile operator facilitates the use of Wi-Fi instead of mobile network access to their subscribers [67] [68], as it Wi-Fi is more cost effective for data [69] [70]. The level of integration can be very different from operator to operator, although up to very recently the integration has been very light or non-existent. This low integration is not sufficient as it misses a lot of opportunities in which Wi-Fi is available but not used because the device is lacking knowledge and it requires user interaction/permission to use the available Wi-Fi network. Most of these Wi-Fi networks also require the subscribers to manually login, this prevents seamless authentication and therefore the complete seamless experience desired [71].

It also depends on who owns the Wi-Fi network the subscribers are advised/recommended to use. This Wi-Fi access can be under the control of the operator, a third-party, or be private Wi-Fi networks which the subscriber has access to.

There are several ways in which Wi-Fi offload access can be made more seamless to the users improving their experience. This topic will be further explained and described in Section 2.6.

Historically, approaches have relied on tunnelling traffic across the Wi-Fi and/or cellular networks to a common core network [72] [73]. Such tunnelling approaches introduce significant cost overheads and rely on device centric features such as Mobile IP and mobile IPSec (Internet Protocol Security). This reliance on device OEMs (Original Equipment Manufacturer) to build features into their handsets met with limited success and has been mostly abandoned.

That does not mean that Wi-Fi offloading is not happening [74], but it has so far not been done rigorously and the integration of Wi-Fi into the mobile network has been very limited. In Section 3.5, an explanation of why integrating Wi-Fi into mobile networks is desired can be found.

3.4.2. LTE

The first LTE networks started deployment in 2011, with trials and PoCs (Proof of Concept) all over the world, see Figure 13. The importance of LTE is that being and all-IP network from the beginning it is more suited to integrate with other data only wireless technologies like Wi-Fi or WiMAX. At the same time, LTE has been the fastest 3GPP's radio technology moving from standard ratification to worldwide deployment, and it has joined the future evolution paths of 3GPP, 3GPP2 and WiMAX mobile networks into a single roadmap.

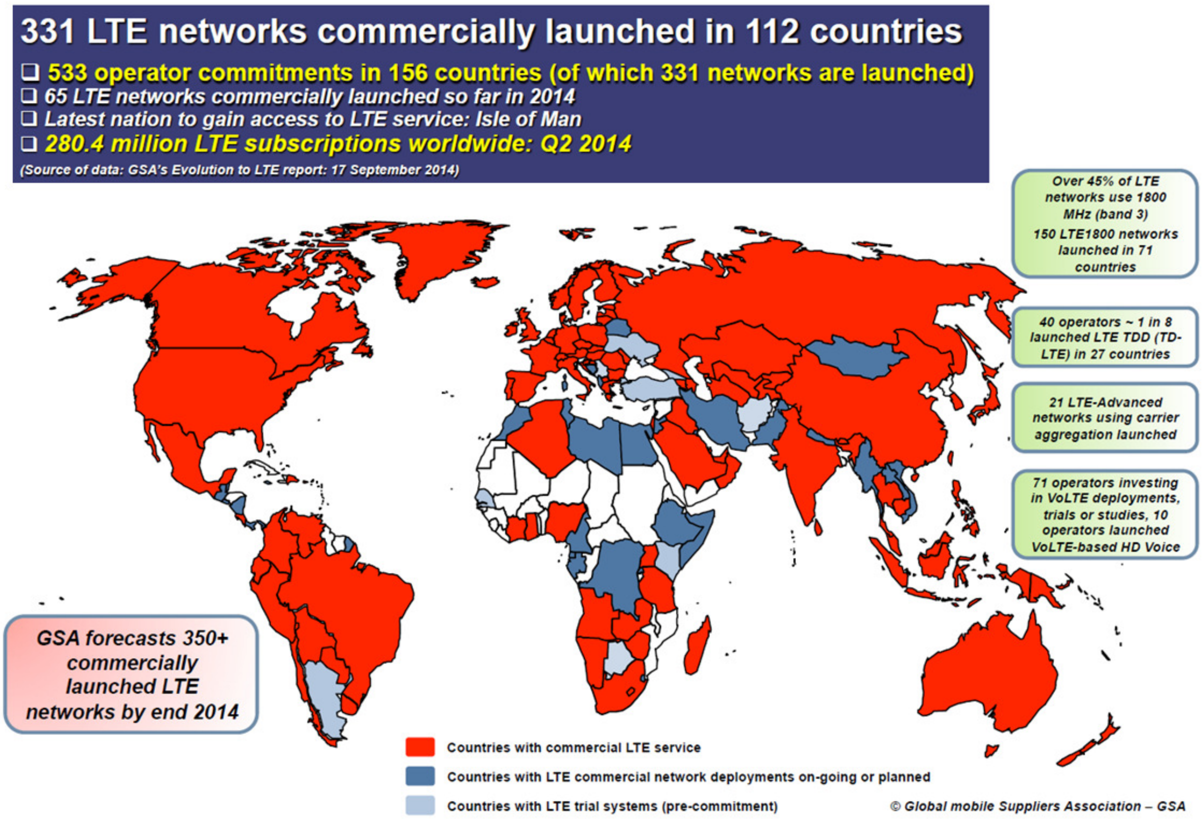


Figure 13 - LTE networks commercially launched by Q2 2014 (Source: GSA- Global mobile Suppliers Association).

The new standard by 3GPP already includes interfaces for the integration of non-3GPP networks both trusted and un-trusted. The definition of trusted access in 3GPP defines a type of connection using interface S2a which can interact directly with the EPC [75], while untrusted access requires using the interface S2b and an intermediary network entity called ePDG (Evolved Packet Data Gateway) [76], its main responsibility to provide security mechanisms (IPSec tunnels) to establish a connection with the subscribers device via the untrusted non-3GPP network. The 3GPP leaves the mobile operator the decision of which connections to consider trusted and which untrusted.

Wi-Fi Trusted Access

Trusted access is usually expected to be a Wi-Fi access deployed by the mobile operator with secure authentication and encryption in the radio access [77]. The following features are also assumed:

- Authentication via 802.1x which means radio access encryption.
- EAP (Extensible Authentication Protocol) authentication for 3GPP-based network access (preferably EAP-SIM/AKA/AKA' (Authentication and Key Agreement) [78]), as it means the same authentication mechanisms used in the mobile network are reused in the Wi-Fi network.

The subscriber device connects through a TWAG (Trusted Wireless Access Gateway), which connects directly with the P-GW (Packet Gateway) in the EPC through a secure tunnel using interface s2a, see Figure 14.

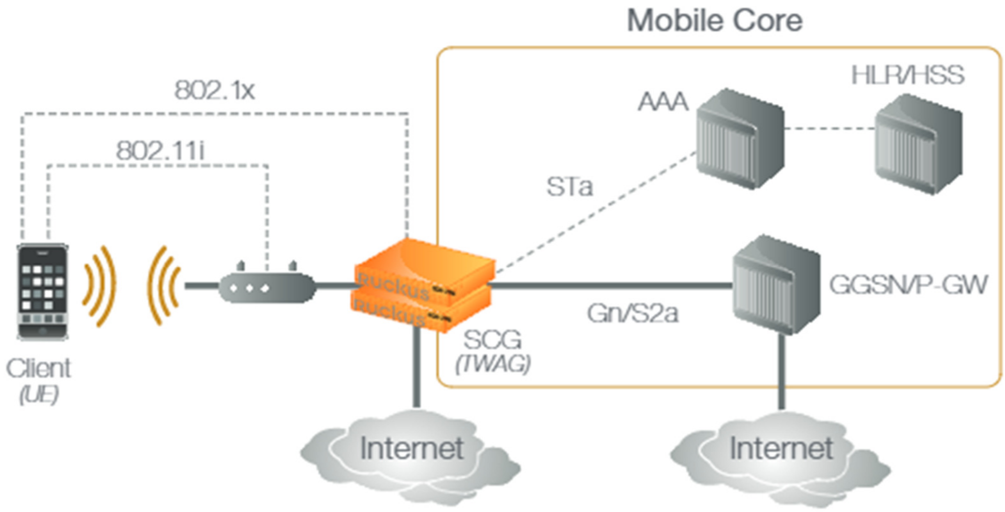


Figure 14 - Trusted wireless LAN access using TWAG functionality (Source: Ruckus Wireless).

Wi-Fi Un-trusted Access

When Wi-Fi was first considered to get introduced in the 3GPP standards (2005), it was not very common to find Wi-Fi access points with advanced security features, so Wi-Fi was labelled by default as not secure. Untrusted access includes all types of Wi-Fi networks and access points in which the mobile operator has no control. In this case, there are no requirements on the Wi-Fi access network, but in the device which needs to be able to setup a secure channel (IPSec tunnel) through the non-trusted network up to the ePDG in the EPC. The ePDG is then connected to the EPC where each user session is channelled inside a secure tunnel [77], see Figure 15.

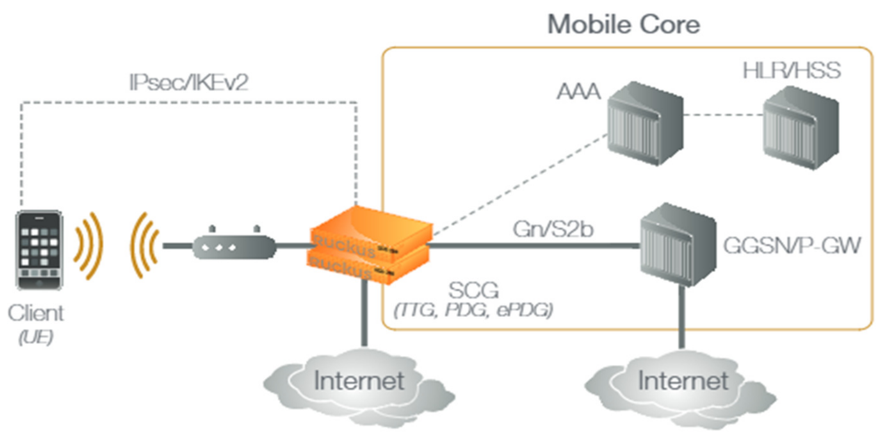


Figure 15 - Untrusted wireless LAN access using TTG, PDG, or ePDG functionality (Source: Ruckus Wireless).

This type of connection allows for any Wi-Fi access to be used to integrate with the mobile network.

3.4.3. Small Cells/ Small Cell Offload

Until 2011-2012 there was a big differentiation on the use and size of different types of low powered mobile network base stations. But after that, the FemtoForum decided to stop the differentiation and cover all under a common umbrella term, "small cells" [79] Inside the term small cells now we can find:

- **Femtocells:** Low power, normally with a range between 10-50 m they use fix broadband connection as a backhaul. In use in the home (8-16 max users), in the enterprise (16-32 max users) and even outdoors in high density scenarios.
- **Picocells:** low power, normally with a range between 30-100 m using fix broadband connection as a backhaul. In use in enterprise with a planned deployment (32-64 max users per cell), outdoors in high density scenarios and in rural areas to provide coverage in no-spots.
- **Metrocells and Microcells:** medium power, range between 100-500 m, using a mix of fix broadband and common backhaul technologies. It is used outdoors for hotspot coverage and in rural areas for no-spot coverage.

Small cells allow the mobile operators to place base stations closer to the subscribers, which in turn increases the amount of spectrum available per customer, improving user experience, throughput (sometimes limited by the backhaul technology available) and decreasing the cost per MB to the mobile operator; especially in those cases where the backhaul is paid for by the subscriber (for example, home femtocells and enterprise femtocells and picocells). By allowing subscribers to connect to small cells, the overall number of subscribers connected in a macrocell area decreases, helping with congestion in macrocell base stations and as a result improving the user experience also for subscribers not in the range/coverage of the small cell.

While in 3G the main reason for operators to deploy small cells was to increase the coverage and reduce congestion, with 4G the main reason is to increase capacity. The new radio technology of 4G allows for a much higher transmission rate, and small cells are one of the options for the mobile operators to provide the capacity that is predicted to be required in the near future. As it is expected that more spectrum in higher frequencies will become available new solutions to deploy high capacity small cells in higher frequencies have started to appear with the name of LTE-Hi [80].

The other advantage from 3G small cells is that 4G is all IP making the deployment of small cells much simpler, especially the integration to the core network where they don't need to provide a special linkage with the circuit switched voice network.

All the above mentioned reasons make small cells a great place to integrate Wi-Fi and 4G as both technologies can share the same links into the core network (although different data path required). It makes easier for the operator to control the usage of the different radios for different applications.

3.4.4. LTE and Wi-Fi Frequency Bands

Figure 16 below illustrates the licensed and un-licensed frequency bands in the 2300MHz to 2700MHz spectrum in the UK.

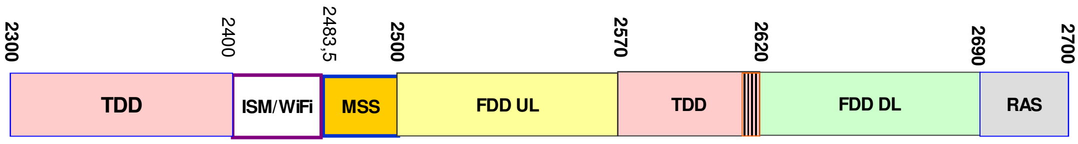


Figure 16 - 2300/2700 MHz band plan (Source: OFCOM).

The 2.4 GHz band is allocated to ISM (Industry, Scientific and Medical), and it is an unlicensed band. In the past, the frequency bands 2300-2400 MHz and 2500-2690 MHz adjacent to ISM Wi-Fi band were used by military systems. 2500-2690 MHz band was allocated to IMT (International Mobile Telecommunications) mobile service at WRC-2000, and 2300-2400 MHz band was allocated to IMT mobile service at WRC-2012.

2300-2700 MHz band frequency arrangement plotted in Figure 16 can be summarised as:

- 2300-2400 MHz: LTE band 40 in 3GPP TS36.104, LTE TDD (Time Division Duplex).
- 2400-2483.5 MHz: ISM band, used by Wi-Fi.
- 2483.5 – 2500 MHz: the band 2483.5-2500 MHz is allocated to the fixed, mobile satellite, radiolocation and radio determination-satellite services. It is used by MSS (Mobile Satellite Service) for the link space to earth.
- 2500-2570 MHz: band 7 in 3GPP TS36.104, LTE FDD UL (Uplink).
- 2570-2620 MHz: band 38 in 3GPP TS36.10, LTE TDD.
- 2620 – 2690 MHz: band 7 in 3GPP TS36.104, LTE FDD DL (Downlink).
- 2690-2700 MHz: Radio Astronomy.

The 2.4 GHz Wi-Fi band is split into 14 overlapping channels of 20 MHz bandwidth with carrier separation of 5 MHz and with centre frequencies shown below. Within the UK only channels 1-13 are allowed, see Table 1.

Table 1 - 2.4GHz channel table (Source: ETSI).

Channel	Centre Frequency	Usage Restrictions
1	2.412	Available in UK
2	2.417	Available in UK
3	2.422	Available in UK
4	2.427	Available in UK
5	2.432	Available in UK
6	2.437	Available in UK
7	2.442	Available in UK
8	2.447	Available in UK
9	2.452	Available in UK
10	2.457	Available in UK
11	2.462	Available in UK
12	2,467	Available in UK
13	2.472	Available in UK
14	2.484	Not in UK, Japan only

The 5 GHz band is divided in 42 different non-overlapping channels of 20 MHz, but the channels allowed in each territory depends on the local regulator (in UK 19 channels are allowed [81]).

3.4.5. UK 2.6 GHz LTE Auction Results

Following the recent UK auction the 2.6GHz band was allocated as shown below in Figure 17:

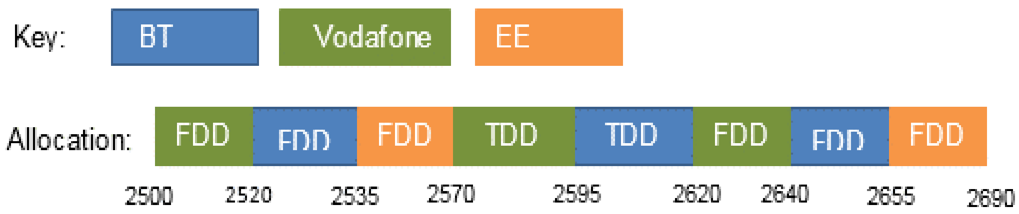


Figure 17 - 4G 2.6 GHz auction results in UK (Source: OFCOM).

As we can see BT has LTE FDD Uplink spectrum in the 2520-2535 MHz band whilst Vodafone has LTE Uplink spectrum in the 2500-2520 band. The guard band between the Wi-Fi channel 11 and the Vodafone band is therefore 2500-2472 = 28 MHz.

The interactions and interferences between those 2 operators LTE UL spectrum and Wi-Fi are further discussed in Section 8.

3.5.Why Integrate LTE & Wi-Fi Networks?

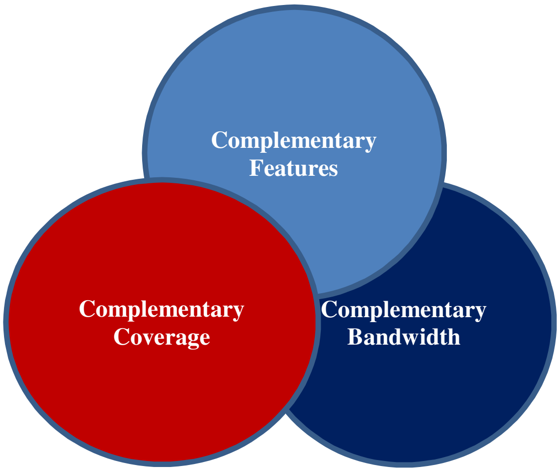
LTE and Wi-Fi networks are in many ways complimentary technologies, together could offer a better overall mobile broadband experience than either technology alone, see Table 2. Wi-Fi ubiquity (one UK mobile operator has around 20000 base stations, while BT Wi-fi has over 8 million) , high throughput (speeds over 100Mbps are common) and large spectrum resource

(400MHz) provide a large capacity for carrying traffic; whilst LTE's guaranteed QoS (Quality of Service), reserved spectrum (interference free or at least controlled), better receiver quality (power control) and secure credentials (via SIM - Subscriber Identity Module) provide an important range and functionality options.

Table 2 - Wi-Fi vs LTE strong point comparison.

Wi-Fi Strong Points	LTE Strong Points
• Lots of spectrum in multiple bands – 400 MHz in total. • Very high bitrates possible >100 Mbps over the air. • Multiple frequency bands 2.4 / 5 / 60 GHz with varying propagation. • Low station power consumption (<100 mW). • Supports mesh networks, using IEEE 802.11s [82]. • Peer-to-peer (Wi-Fi Direct) as well as base station operation modes. • Low cost network infrastructure. • Simple pairing mechanisms e.g. NFC (Near Field Communications), Push button .	• Reserved spectrum – limited interference. • Network controlled resource scheduling, Admission control. • Higher station TX (Transmission) power limits - increased range. • Session mobility to the macro network. • Standardised real-time services. • Advanced features – Coordinated Multi Point (CoMP), Beam-forming, Multicast (eMBNS, Enhanced Multimedia Broadcast Multicast Services). • Network paging modes • Standardised credential – SIM

Combining these strengths well would clearly offer the potential to deliver new classes of mobile broadband services and potentially a differentiated mobile customer experience, see Figure 18.



<u>Complementary Throughput – combining the throughput of the two radios</u>
Throughput is additive since spectrum is independent
Throughput variation with time and space independent.
<u>Complementary Coverage - combining the different coverage areas</u>
Different frequency bands & power levels.
Different antenna patterns.
Different handling of inter-cell handover.
<u>Complementary Features- combining the feature sets</u>
Scheduled + Unscheduled Access.
Multipoint transmissions.
Peer to peer mechanisms.
Session mobility and handover.

Figure 18 - Wi-Fi and LTE, complementary technologies.

Two groups of service scenarios are most often considered when looking to combine the two radios:

- Improved throughput.
- More reliable connections.

These two scenarios place different requirements on the integration architecture which we will look at in Section 3.6.

The combination of Wi-Fi and LTE, known as bundling or IP flow mobility, is used to increase the bandwidth that can be delivered to a single user while utilizing the current network infrastructure to the maximum, allowing dual simultaneous usage of Wi-Fi and mobile networks. The main drawback of using this technique is higher energy consumption [83] due to the fact that 2 radios are actively sending and receiving data [84]. Devices need to be able to decide which data to send over Wi-Fi and which over the mobile network. Devices currently only use one or the other, and support for more than 1 simultaneous radio is non-existent in current commercial deployments.

There are 2 main scenarios:

- Same AP: does not make sense in good radio conditions when the delivery is from the same access point (with dual radio, like a small cell in an office or a house) as the bandwidth that can be delivered is limited by a single backhaul to the access point, but in a challenging radio environment, the bandwidth delivered by any of the 2 technologies could be inferior to the backhaul available and therefore there would be a gain from using both radios at the same time. In this case, the control can be done directly at the AP without wasting core network resources.

- Different APs: the mobile network AP and the Wi-Fi AP are different and because the backhaul for each is completely independent of the other a higher output can be achieved. This also allows for smoother handovers between Wi-Fi Hotspots and between mobile networks as the radios are always on and the end user device can always be reached. The drawback is that this solution requires more processing in the core network and in the device.

There are several standards/working groups and individuals that have been working on this field, for example, the IETF (International Engineering Task Group) MONET (Mobile Networks)/NEMO (Network Mobility) working group [85] , the IETF GRE notifications working group [86] and universities [87].

3.5.1. Combining Wi-Fi and LTE for Improved Throughput Services

Combining Wi-Fi and LTE for improved throughput can cover a range of possible implementation requirements. On a modern smartphone/tablet it is common for many applications to be running in parallel often with vastly different connection requirements. Maximising the user mobile broadband experience can therefore imply different approaches:

- Maximising aggregate bandwidth across a number of parallel connections or applications.
- Enabling QoS and non-QoS application co-existence.
- Enabling a single high bandwidth TCP (Transport Control Protocol)/IP connection.

The first two approaches require the ability to distribute IP flows across the two radio networks to either globally maximise throughput or to leverage differing QoS capabilities of the two technologies, whereas the last looks to deliver packets from within a single IP flow across multiple networks to enable, for example, a HD video streaming client.

Example#1-Aggregate Bandwidth Best Effort Service

An example of such a service would be the RapidSync scenario (BT Internal test tool). This application provides peer-to-peer file synchronisation between multiple devices using the BitTorrent protocols. BitTorrent protocols distribute files across multiple peers and clients can open multiple IP sockets to multiple peers in order to download content in parallel from multiple peers. By distributing the BitTorrent UDP (User Datagram Protocol) sockets across multiple radios we would deliver a higher aggregate bandwidth and therefore faster synchronisation.

Example#2-QoS and Non-QoS Dependent Service

A typical example would be a multimedia conferencing service where QoS dependent VoIP traffic would always be routed via the LTE network whereas the higher bandwidth desktop sharing component will be maintained over the Wi-Fi network, see Figure 19.

Key to enabling high bandwidth services is therefore the ability for an operator to control how traffic is distributed across the two radio networks.

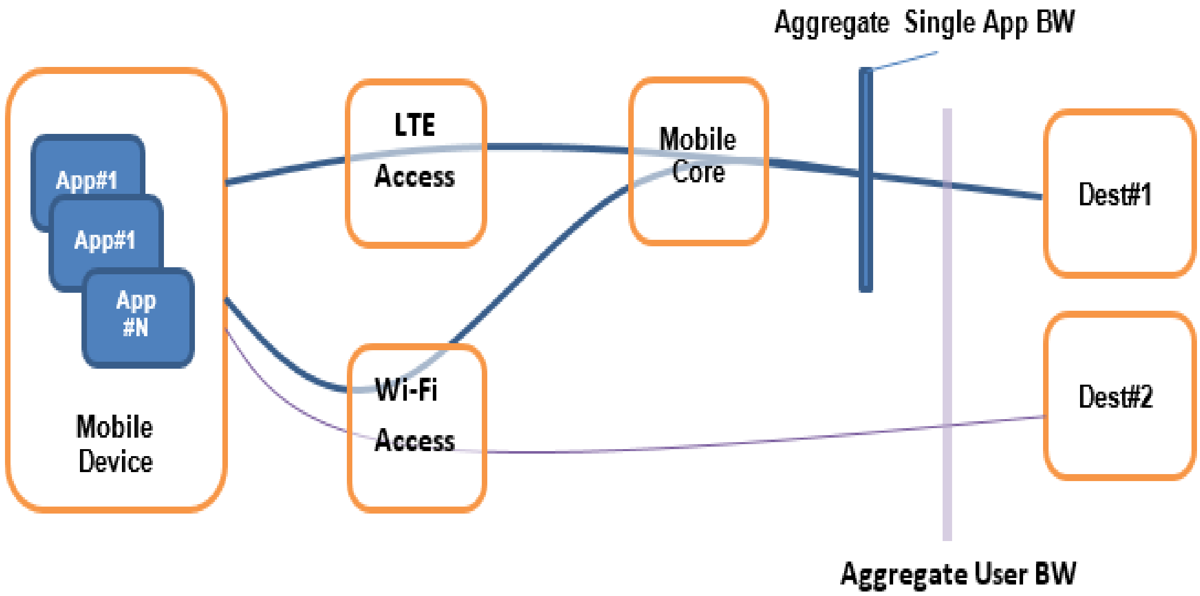


Figure 19 - Combining Wi-Fi and LTE radios for aggregate throughput.

3.5.2. Combining Wi-Fi and LTE for Improved Coverage/Reliability

Of particular interest for small cell indoor LTE networks is the option of combining these two radios to exploit their potentially differing radio propagation to deliver a more reliable connection.

When combining radio technologies for coverage applications then the key requirement is that applications should not be interrupted when traffic is moved from one network to the other (as long as there is an available radio to attach to). In other words, the key requirement here is that handover between the two radios should be transparent to the user.

Example#1- Continuous Seamless Coverage Using Wi-Fi/LTE

The example here is based on the idea that coverage would not be ubiquitous for any single technology but there will always be at least 1 radio technology available. The device then with the help of the network needs to be able to handover between each of the technologies without interrupting any sessions.

3.6.Current Integration Enabling Technologies

To achieve the level of integration required between LTE and Wi-Fi networks with a coherent user experience in a cost efficient way, we have to rely on end-to-end standard based solutions that involve both the core network and the end-user devices.

Recently the industry has focused on network centric approaches which exploit security enhancements in emerging 'carrier grade' Wi-Fi networks as well as new features enabled by LTE core cellular networks to enable Wi-Fi and LTE radios access to be treated equivalently by the mobile core. This approach enables a range of integration implementations able to support legacy devices unchanged.

Key to these approaches is the role of the LTE Evolved Packet Core as the common core network for an integrated Wi-Fi/LTE mobile broadband service.

In the next Sections (3.6.1, 3.6.2, 3.6.3, 3.6.4) the main current and emerging technologies/standards trying to increase the level of integration, usability and seamlessness between Wi-Fi and mobile networks will be reviewed.

3.6.1. SaMoG (S2a Mobility over GTP)

The 3GPP SaMOG study group have defined a roadmap of features progressing from basic integration of Wi-Fi access with the cellular core through to seamless handover between Wi-Fi and LTE networks and to ultimately include replication of LTE features such as multiple APN support and IP Flow mobility. The end goal is to make the Radio Access Technology transparent to the mobile core and therefore transparent to services and user experience.

The SaMOG group defines these features along the usual 3GPP release cycle. SaMOG Release 11 supports:

- Simultaneous Wi-Fi and LTE provided different APNs (Access Point Name) are used for the LTE and Wi-Fi networks.
  - Because different APNs are used, different IP addresses are allocated to each interface.
- Wi-Fi traffic can be routed via the EPC or can be routed out to the internet by the Wi-Fi access network (NSWO, Non-Seamless WLAN Offload).

The 3GPP Release 11 SaMOG activity extends previous 3GPP Release 8 work on trusted non-cellular access to the EPC (TS23.402). It explicitly defines the requirements for devices and networks where the non-cellular access network is Wi-Fi and where the goal is to ensure no modifications are necessary to the device. To achieve this goal the SaMOG approach requires a separate Wi-Fi Specific APN or P-GW to be used. There is no common anchor point for LTE and Wi-Fi traffic and therefore no option for seamless handover between Wi-Fi and Cellular.

In addition to formalising the use of Wi-Fi as a trusted non-3GPP access network, SaMOG also introduced the option of GPRS Tunnelling Protocol as the mobility signalling and data transport protocol between the Wi-Fi Access network and the Evolved Packet Core.

Fundamental to the SaMOG architecture, see Figure 20, is the introduction of the TWAG function within the Wi-Fi access network. In order to support the goal of enabling Wi-Fi to simply become another radio access to a common mobile core, then the TWAG requires a Layer 2 connection to the mobile device. This requirement does place additional requirements on the Wi-Fi access network.

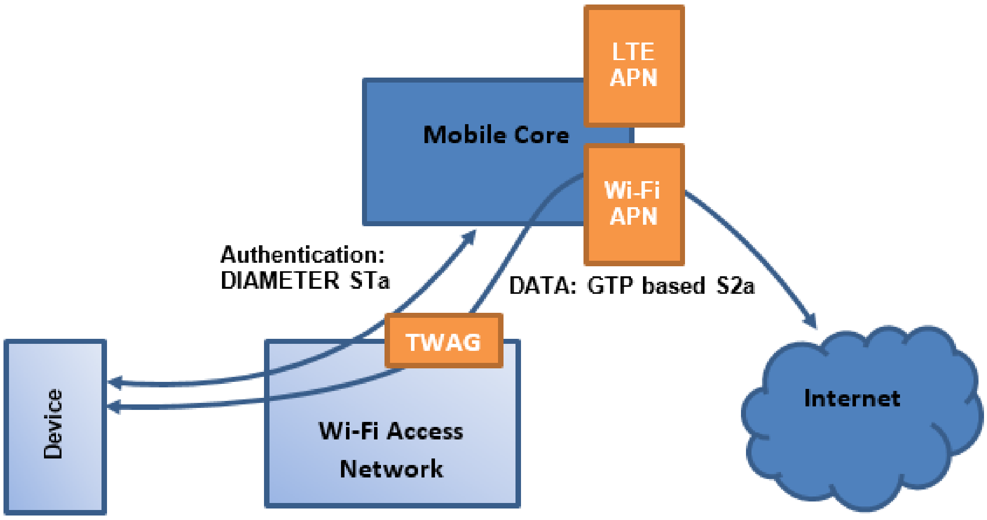


Figure 20 - SaMOG trusted Wi-Fi access, requires modification to Wi-Fi access network only (Data Source: 3GPP).

Supporting Breakout Traffic in SaMOG

Even when it is possible to integrate Wi-Fi and LTE within the same network, it is not always necessary or desirable from a customer experience or cost effectiveness perspective for all the Wi-Fi user traffic to be routed via the EPC. Where traffic is low value and perhaps doesn’t require special features such as QoS or handover then it can be better to break this traffic out directly within the Wi-Fi access network. SaMOG supports this concept as NSWO (Non-Seamless WLAN Offload). In Release 11, NSWO cannot be active at the same time as core routed Wi-Fi, however this restriction is removed in Release 12.

Supporting Seamless Handover in SaMOG

SaMOG Release 11 assumed a requirement for no device firmware changes which came at a cost in terms of functionality. Whilst Release 11 SaMOG architecture allows for Wi-Fi data traffic to be routed via the EPC, it does not allow seamless handover between cellular and Wi-Fi networks. All Wi-Fi traffic will be routed to a separate logical APN within the EPC. Applications will therefore not maintain their IP address if the device switches between LTE and Wi-Fi access networks.

To achieve seamless handover requires changes to the way the device IP stacks behave. Whilst these changes are minimal and much easier to implement than the historical tunnelling based approaches, mentioned in Section 1, nevertheless seamless handover still requires device support. Specifying these changes has been completed within SaMOG Release 12.

SaMOG Release 12 therefore adds:

- Session mobility between LTE and Wi-Fi with IP address preservation for a common APN.
- Support for MAPCON (Multi Access PDN Connectivity) over Wi-Fi
    - Requires a new signalling mechanism between the UE (User Equipment) and the Wi-Fi network.
- Support for simultaneous traffic routed via the EPC and via non-seamless WLAN offload at the same time when connected to the same SSID (Service Set Identifier). It is envisaged that the SSID will be used as an indicator to the UE as to whether it is connected to the EPC or not, so that the UE can decide whether applications that are incompatible with EPC core routing e.g. local DLNA services are usable on this Wi-Fi network.

Supporting Multiple APNs over Wi-Fi

In order to support advanced LTE features such as MAPCON over Wi-Fi access, the SaMOG standards needed to introduce new mechanisms to enable the mobile device to request new APNs (with and without handover) as well as to be able to maintain multiple IP addresses over the Wi-Fi network, see Figure 21.

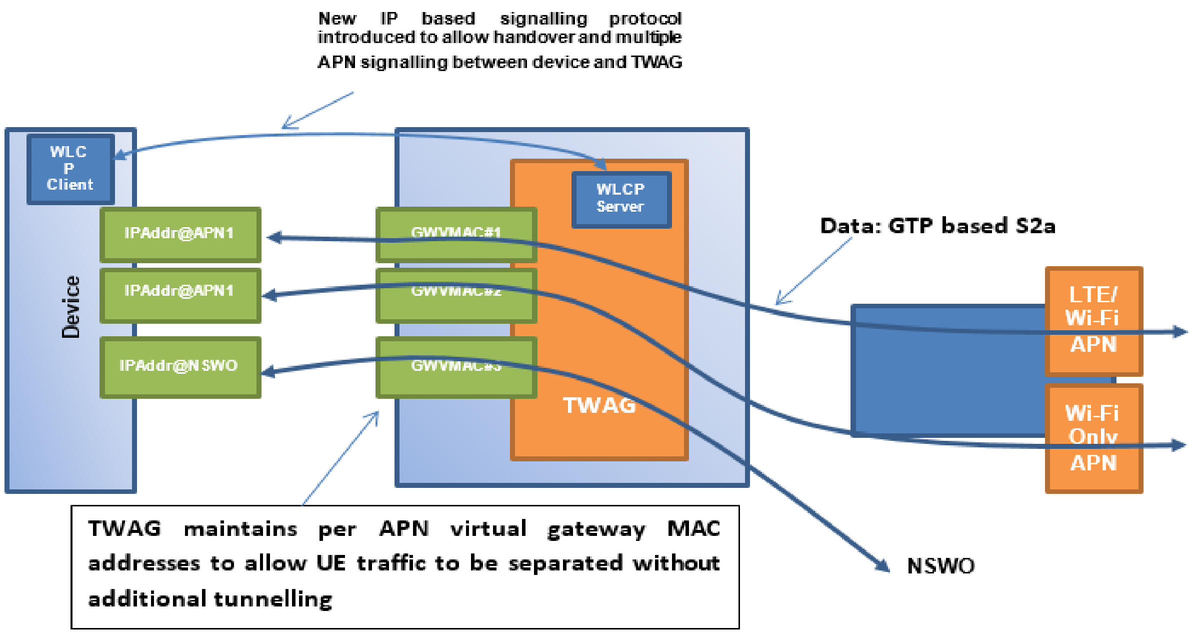


Figure 21 - SaMOG R12 multi APN support (Data Source: 3GPP).

To avoid the overhead of tunnelling, the proposed Release 12 introduces a new IP layer signalling protocol, WLCP (Wireless LAN Control Protocol), which is used to request the TWAG to create S2a GTP (GPRS Tunnelling Protocol) tunnels to secondary APNs. The TWAG node is also extended to support multiple virtual gateway MAC (Media Access Control) addresses allowing each APN to be allocated a different GW address. This enables separation of per APN traffic without the overhead of tunnels.

At this point in time the SaMOG Release WLCP protocol has yet to be formally specified and agreed.

3.6.2. ANDSF

Once we allow a device to be simultaneously connected to both Wi-Fi and LTE networks, we need mechanisms to control how traffic is routed across the two networks. The only 3GPP mechanism available to control the on-device traffic routing policies is defined by the 3GPP ANDSF specification.

ANDSF is a function specified by the 3GPP in R8 and more recent of TS 23.402, TS 23.302 and TS 24.312 with the purpose of assisting the subscriber's device to discover nearby non-3GPP networks (Wi-Fi, WiMAX) and provide the traffic routing policies that the operator would like to use to distribute traffic across non-3GPP/3GPP networks.

ANDSF requires either native support in the device or a connection manager installed with support for it. At the moment from the main manufacturers only Samsung has announced it will be added in their next device releases (2015).

ANDSF can use all the network intelligence from the mobile operator in terms of (congestion, time of day, roaming agreements to nearby hotspots,…) plus the specific situation sensed from the user equipment (battery levels, signal strength, location,…) to take decisions on which network is more suitable to fulfils the subscriber's needs. ANDSF defines:

- Policies for 3GPP devices to decide which Wi-Fi network to use and when – Inter System Mobility (see Table 3).
- Policies for which traffic is routed over which access network – Inter System Routing (see Table 3).

Table 3 - ISMP (Inter System Mobility Policies) and ISRP (Inter System Routing Policies) comparison (Data Source: 3GPP).

ISMP	**ISRP**

• Access network level policies
• When to use Wi-Fi vs Cellular
• Which Wi-Fi network to use and when ordered by
    ○ Time of day
    ○ Location
    ○ SSID
	• Traffic level decisions
	• Which traffic over which radio
	• Traffic can be identified by
	    ○ APN
	    ○ IP n-tuple : src IP/port, dest IP/port
	    ○ Application type
	• Different rules can be applied when roaming

NOTE: a Visited ANDSF may override home network rules

To date, the ISRP rules allow an operator to specify rather high level routing policies, for example which applications will run over LTE and which will run over Wi-Fi. Work is ongoing within the 3GPP to further refine these Inter-System Routing Policies to allow finer grained control of the traffic routing. The OPIIS (Operator Policies for IP Interface Selection, defined in TR23.853) working group is defining extensions to the ISRP policies in ANDSF to introduce IARP (Inter-APN Routing Policy) which allows prioritised list of APNs to be applied to traffic flows.

- Traffic flows identified by IP-Tuple.
- Allows specific IP Traffic flows to be directed to a particular APN.
  - e.g. Separate APN for IMS (Internet Multimedia Subsystem) Services
- Simultaneous Wi-Fi and cellular APNs

In addition, the 3GPP WLAN Radio Interworking Group TR37.834 is extending the ANDSF policies to allow more localised distribution of policies to the mobile device. The goal here is to allow the access network to push local ANDSF based routing rules to devices in response to, for example, changes in localised congestion or radio conditions. Again the aim here is to enable the operators to control which radio is used for which application on a per user basis so that the customer experience is maximised, see Figure 22 - Future device connection scenario (Data Source: 3GPP)..

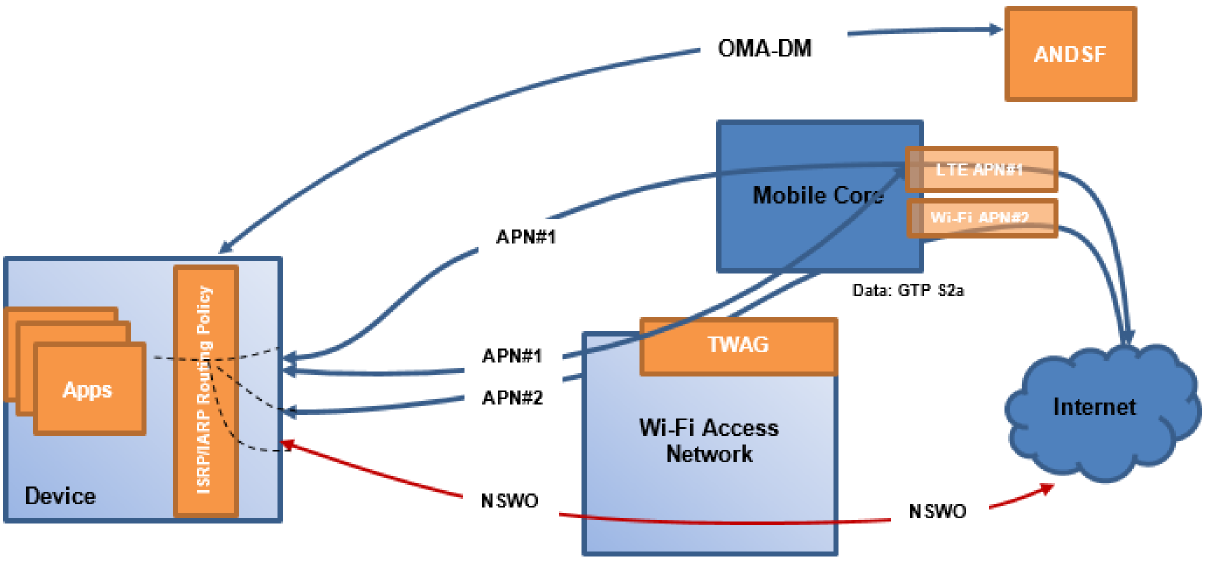


Figure 22 - Future device connection scenario (Data Source: 3GPP).

In future, therefore, we can envisage a mobile device being connected to Wi-Fi and LTE with multiple APNs over each radio and with combinations of mobile core routed traffic and breakout (NSWO) traffic where complex traffic rules are required to provide the correct customer experience.

3.6.3. 802.21/MIH

In 2007 many had noticed that current devices in order to be able to use the different types of wireless networks available needed to discover them first, intelligently select the most appropriate one for the current conditions, authenticate and optimize the handover to the new found network. The IEEE decided to create a working group to study the subject and 802.21 workgroup started with the premise of "enable the optimization of handover between heterogeneous IEEE 802 networks and facilitate handover between IEEE 802 networks and cellular networks", see Figure 23.

802.21 [88] aka Media independent handover was ratified by IEEE in 2009. This standard enables seamless handover between networks of the same type and between different network types, which are called MIH or vertical handover. The standard provides information to allow handing over to and from 802.3, 802.11, 802.15, 802.16, 3GPP and 3GPP2 networks through different handover mechanisms.

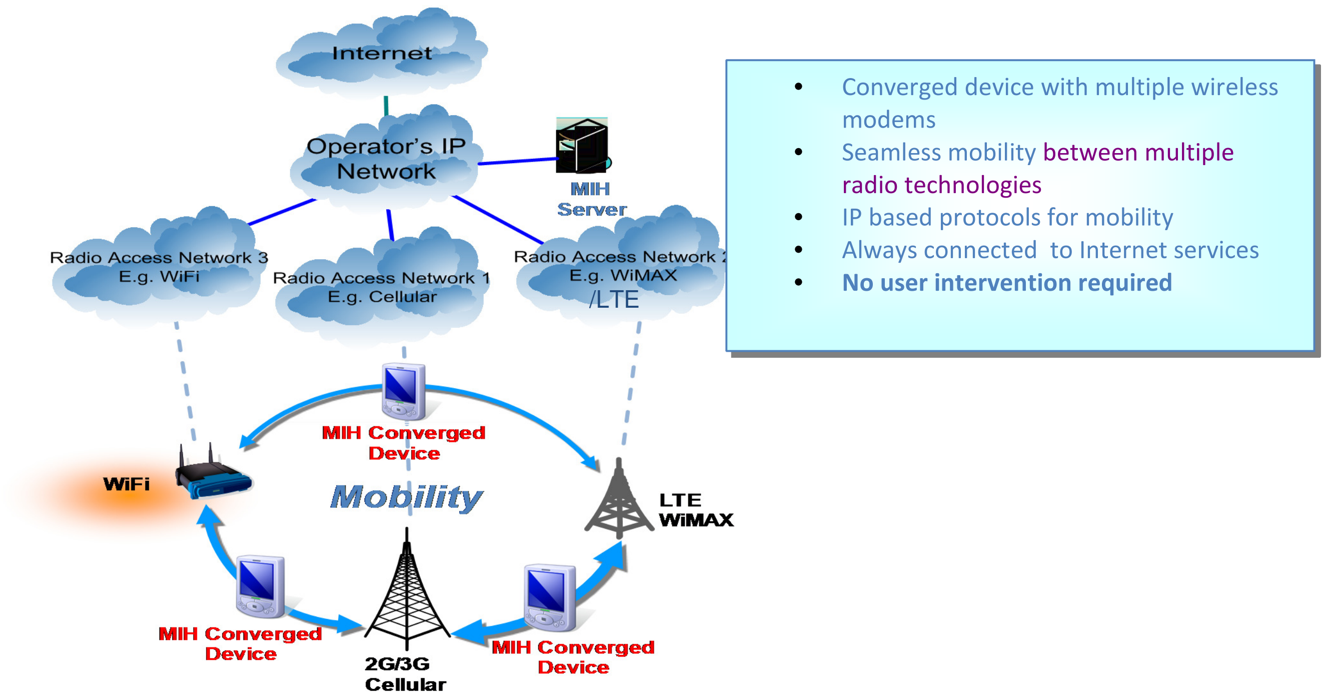


Figure 23 - 802.21 (MIH) principles (Source: BT).

802.21 is composed by 3 different services:

- MIIS: similar to ANDSF, the MIIS provides the ability for devices to gather a list of IEs (Information Elements). These IEs provide information about all networks and their PoAs (Points of Attachment) if needed. It uses the bearer link to retrieve information from an IS (Information Server) on the network, regarding other networks available.

When using MIH the device knows where to expect coverage for a given Wi-Fi hotspot, it builds a networks map using the IEs. More importantly, since this information is retrieved in advance and using the bearer link (e.g. 3G) the device does not need to perform periodical scanning and may switch off altogether the radio interfaces that it does not need in an area. This leads to significant power savings, which are highly important on a mobile device to maximize the life of its battery. When the device reaches a location where it believes Wi-Fi coverage is available, it switches ON the Wi-Fi interface and performs a limited scan, to make sure that the access point coverage is actually in place. The scan performed is “limited” because the IEs specify channel, SSID and all details needed for the device to be able to connect to the hotspot as soon as possible.

- MIES (Media Independent Event Service): Delivers events from the link layer (usually link quality and status) to the upper layers within the device or network (local and remote interfaces). By using the Event Service (ES), the device is notified about a number of events as they happen. Probably the most important one is the “LINK GOING DOWN” event. This means that the device will be notified, in advance, about the coverage of the Wi-Fi hotspot being lost. The device may, therefore, prepare a handover to another technology (LTE if in coverage) before the signal is actually lost. In order to support this functionality devices run within the MIH client deployed on them a “smart triggering” solution. These smart triggers are algorithms that predict the signal being lost to a given degree of accuracy. The better the algorithm is, the better the service will work. When a signal loss is predicted the information is passed to a “Connection Manager” component that will have to decide what to do; what new network to connect to (if any).
- MICS (Media Independent Command Service): Offers the capability to control and manage the link layer and perform Handovers between the different radio technologies of the device. The Command Service is the component that actually provides support to order connection/disconnection from networks (at physical layer, this is). This process may be based on significant signal fading (LINK GOING DOWN detected, one of the Events) or on a handover decision taken by a Connection Manager component. An example of this behaviour might be the detection of a preferred network available when connected to another.

In this sense, intelligence or decision making regarding what connection to choose at any moment is deployed in a Connection Manager component, which can be placed at the device or the network [89].

Currently none of the major device manufacturers or chipset vendors have announced any intention to support 802.21, but a lot of different systems have been proposed with MIH as the base for optimized wireless heterogeneous networks [90] [91] [92] [93].

3.6.4. 802.11u & Hotspot 2.0

802.11u (published in February 2011) is an addition to the 802.11-2007 standard to include features that improve the interworking with mobile networks.

802.11u provides information like:

- Type of access (Private, free public, for-fee public).
- Roaming consortium.
- Venue information.
- AP domain name.
- Roaming partners allowed with EAP authentication method supported.
- IP address type.

To provide this information 802.11u uses GAS (Generic Advertisement Service) and ANQP (Access Network Query Protocol) which are used by the mobile device to access the information directly from the hotspot, via ANQP, or from the mobile network, via GAS.

802.11u is being rolled on many Wi-Fi networks and the Wi-Fi Alliance has added it to their "Wi-Fi certified Passpoint", which is also known as Hotspot 2.0 in the industry. Hotspot 2.0 allows a similar roaming experience to mobile networks in the Wi-Fi world, together with seamless authentication.

These two technologies together allow for a more intelligent/seamless handover to Wi-Fi under the control of the device connection manager.

IOS devices that support IOS 7 or newer, Samsung S4 or newer, and other smartphone devices have already been Passpoint certified.

3.7.Future Wireless Environment

The future wireless environment is going to try to maximise the amount of capacity per user [94], the availability of high quality connection and the latency of the connection [95]. To do that smaller cells and in higher density are needed which will increase the amount of HO (Handover) needed [96]. Spectrum usage both in license and unlicensed frequencies will be required to deliver the predicted speeds, and interaction between Wi-Fi and the mobile networks will become a key factor for the success of 5G [96]. At the same time network architecture will change towards virtualization of network functions, management and orchestration [96].

These mainstream thoughts aim all at solutions that are achievable especially in highly populated areas, see Figure 24, but … what happens in rural and semirural areas? How do you provide the same level of service in more difficult to cover areas, planes, trains for example?

Is the subscriber data secure end to end even when switching networks? How fast is the handover between different technologies? Is it seamless to the user? How do you select which networks to connect to, what if they are congested? As different technologies use contiguous spectrum and some of the deployment of these base stations is not controlled (Wi-Fi Aps, and small cells under 100mW), will interference between these technologies be a problem as the density increases?

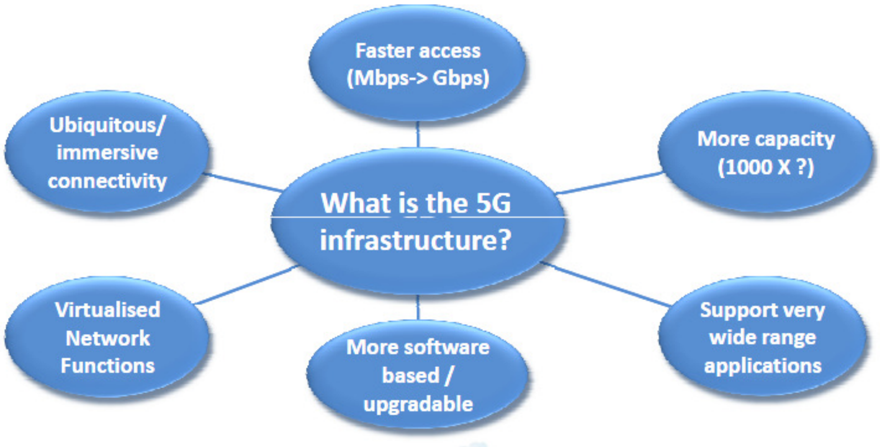


Figure 24 - 5G infrastructure requirements (Source: ETSI Future Mobile Summit).

In the next section the author describes some challenges which to his opinion haven't been sufficiently explored yet, see Figure 25.

3.7.1. Challenges

Description of some of the challenging scenarios identified during the last 4-5 years while working in BT:

Challenge 1: Seamless access to Wi-Fi networks while maintaining mobile operator control, OEMs don't seem to be very supportive. Addressed in Section 4.

Challenge 2: Seamless session handover when moving between Wi-Fi to mobile networks. Addressed in Section 4.

Challenge 3: Wi-Fi network discovery. 802.21 MIH and ANDSF propose 2 similar solutions in which the mobile operator can inform devices of nearby known Wi-Fi networks the device can connect to. This requires a device connection manager that can follow these suggestions and seamlessly handover to the most adequate connection.

Challenge 4: To lower latency, content needs to be much closer to the subscriber, avoiding transfer delays. Network needs to be aware of content location to deliver it in the most efficient way. Addressed in Section 6.3.

Challenge 5: Untrusted Wi-Fi authentication and man in the middle attacks. If the device has not previously connected to a specific network, authentication in open Wi-Fi networks allows traffic to go unencrypted over the air interface. Addressed in Section 5.3.

Challenge 6: Number of small cells can quickly over pass the number of macrocells and their management can create congestion in the core network.

Challenge 7: Interference of LTE bands contiguous to 2.4 GHz Wi-Fi due to low quality radio filters in Wi-Fi devices.

Challenge 8: 2 or more MNOs (Mobile Network Operators) share of RAN (Radio Access Network) resources to decrease the cost of mobile network deployment. Coverage of less densely populated areas might mean lower investment as the returns might not be sufficient. Addressed in Section 7.

Challenge 9: Provision of access in scenarios with a relatively dense number of subscribers but difficult access. The aim is to provide consistent seamless experience wherever you are. Addressed in Section 7.3.

Challenge 10: The main issue with femtocells and picocells is that voice traffic, as explained in [9], is not prioritized over the fix backhaul by default, and although voice traffic is not the most used service (data minutes on mobile are higher than voice minutes) it is the one that customers expect to work flawlessly.

Challenge 11: Wi-Fi currently has higher priority when switched on in the device than mobile networks, which means that data will be forwarded first to any Wi-Fi network detected, avoiding the use of femtocells and picocells. This can hamper the user experience as some Wi-Fi networks might be out of the control of the mobile operator, and it could be in different scenarios the mobile operator would prefer to send the user data via a different radio. In this case a better network selection process is required.

3.8.Proposal – QoE Framework for Wireless Heterogeneous Networks

As we saw in Section 2.1 and Section 2.7, 5G is moving towards seamless network utilization with a combination of licensed and unlicensed spectrum usage, lower latencies and higher bandwidths.

To provide a complete service that can deliver the seamless QoE expected in 5G networks [97] within the available wireless networks to the mobile operator, several different technologies need to be fully assimilated and integrated both in the network operator world and the device ecosystem. When using different technologies (small cells, Wi-Fi or different flavours of 3GPP mobile networks) the ideal subscriber experience means zero touch seamless service continuity, the subscribers do not need to know which type of network they are connecting to or do anything to connect to it, the device and mobile operator need to interact to offer the best possible service in a seamless way.

At the same time to maintain the QoE in the maximum available locations, ingenious solutions need to be found to deliver the right amount of bandwidth and service at the right cost in some of the most hard to reach/cover wireless environments.

Because of this, it was decided to look at all these technologies that help move towards zero-touch and seamless integration between Wi-Fi and mobile networks, while taking into account coverage on the most challenging environments, with the subscriber user experience as the main focus.

The key areas that became the focus of this thesis research are:

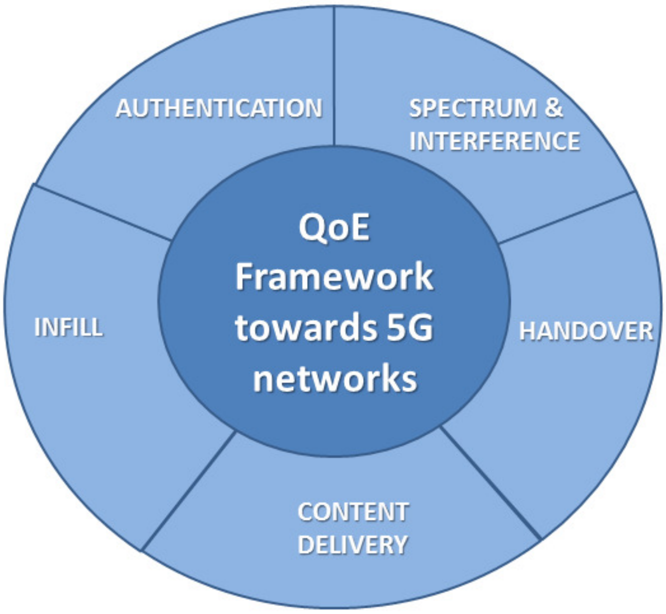


Figure 25 - QoE framework towards 5G networks.

- **Handover:** How do you select which network to connect to? How do you perform a seamless handover to that network? Is this decision in control of the device, the network or is it a collaboration?
- **Security and Authentication:** How can security over Wi-Fi be improved? How can seamless authentication be integrated in current Wi-Fi networks? Can you reuse mobile network authentication?
- **Content delivery:** How do you improve on the existing latencies? Can you push content to the edge of the network? Does it improve the QoE?
- **Infill:** How can a MNO deliver the same or similar QoE that is delivered in urban locations (high availability, coverage, bandwidth, low latency) in areas where there

are not enough subscribers to make it economically viable (rural and semi-rural)? How do you provide service on more challenging scenarios (plane, trains)?

- **Spectrum/Interference management:** What other spectrum will become available in the future, does it need to be so tightly licensed? Does interference exist within the current mobile spectrum and Wi-Fi?

It is expected that the integration of these areas of study will bring current networks closer to the 5G ideal scenario of higher throughput, lower latency, seamlessness, and security.

Chapter 4: Handover

With the coexistence of Wi-Fi and mobile networks in the same environment a graceful handover between the 2 technologies takes extra importance. To achieve it, knowledge from the surrounding wireless network environment is required. Furthermore, as overlapping coverage is expected, the status of such networks (congestion, maximum speeds,..) is also needed, so the device can decide whether moving to a new wireless network would improve or decrease the current service experienced by the subscriber and act accordingly.

Handovers between 4G and 3G, especially between packet switched voice and circuit switched voice, are also key to deliver a seamless service when moving between 4G and 3G coverage, but this problem has already been solved, long studied and optimized by the use of CSFB (Circuit Switched FallBack), SRVCC (Single Radio Voice Call Continuity), eSRVCC (enhanced Single Radio Voice Call Continuity),,.... The recent inclusion of VoWi-Fi (Voice over Wi-Fi) to some commercial networks also implies this HO scenario from packet voice to circuit voice would need to be addressed.

4.1. State of the Art (2009)

The fact that not a managed handover exist between mobile networks and Wi-Fi has been widely discussed [98] [99]. Most of the existing solutions rely on SIP for the handover as it is expected 4G voice will be IMS based [100] [101]. These solutions though don't offer any aid to the device or the operator on how to select to which networks to connect, although there are many proposed algorithms which require a network map or some source of local network information [89] [102] [103] [104]. This issue was discussed in IEEE (2004), and a new working group was started to develop and standardise 802.21 with the aim of providing information to allow seamless handing over to and from 802.3, 802.11, 802.15, 802.16, 3GPP and 3GPP2 networks through different handover mechanisms and algorithms.

Initially the single planned subject for the doctorate was the following: "The study and creation of a network connection manager for all the wireless networks that would work with the still evolving 802.21, aka MIH, functions in the network and MIH compatible devices to steer, advise and/or select the most adequate network for each device usage depending on the current needs".

Some of the first steps in promoting 802.21 were given and one of the first standard compliant MIIS was developed as a result of the study, see Section 4.2.

Nevertheless, during the research period other interlinked subjects were found to require investigation and were subsequently added to the thesis.

4.2.BT MIIS in FMCA First 802.21 Interoperability Event.

An MIIS was developed following 802.21 and was used in the first IOT (Interoperability Testing) tests done by the FMCA in Sophia Antipolis under the ETSI (European Telecommunications Standard Institute) Lab environment [105] [106]. Previous testing had been done on a one to one basis with Intel, NSN, Interdigital and KT (Korea Telecom), and also several versions following the different drafts of the standard had been produced from draft 4 onwards. The MIIS is comparable in the basic functionality with ANDSF, which is what has become more deployed in current mobile networks, see Sections 3.6.2 and 3.6.3.

See in Table 4 the use cases defined by FMCA to test the standard and in Table 5 the test cases mapping to the use case previously defined.

Table 4 - FMCA use cases for ETSI IOT 2009.

Use Case	Title
FMCA-UC1	Network controlled access technology selection
FMCA-UC2	3G to WLAN Handover
FMCA-UC3	Per-flow
FMCA-UC4	Resource limited backhaul
FMCA-UC5	Seamless handover and service adaptation
FMCA-UC6	Adaptive Handover for Application
FMCA-UC7	Multiple Simultaneous Sessions (Data, Voice & Mobility)

Table 5 - FMCA test cases for ETSI IOT 2009.

Test Case	Test Case Description	FMCA Use Cases
FMCA Test Case 1: Network assisted device handover from WCDMA to WiFi using information service	MN query for WiFi radio availability via the 3G network link. MN attaches to the WiFi using the IS query result.	FMCA-UC1, FMCA-UC2, FMCA-UC3, FMCA-UC4
FMCA Test Case 2: Mobile initiated device handover from WiFi to WCDMA triggered by degradation of WiFi signal strength	Based on specific criteria, the MN connects to a different network. Criteria: • WiFi signal strength deteriorating (e.g. from WiFi to 3G), • Device location (GPS) information update: based on a previous IS query indicates that a better service is now available (e.g. 3G to WiFi), • User software application indicating and triggering connection to a new access technology (e.g. WiFi to 3G).	FMCA-UC6
FMCA Test Case 3: Network Initiated Handover	Precondition: Network contains the location information of the MN The PoS commands the MN to handover to connect to a specific PoA.	FMCA-UC1, FMCA-UC4, FMCA-UC5

In the 3 test cases in Table 5 the BT MIIS was used (the only other developed MIIS was by KT which did not support some of the optional fields) and although there were some minor issues on the understanding of the standard which were later clarified in the following standard releases (bit ordering in bitmap, for example), the BT MIIS managed to successfully rely all the required information to all the MIH clients it connected to (see Annex A for examples of decoded MIH messages)

The other participants in this first 802.21 IOT were: Telcordia, Interdigital, KT, Toshiba, Samsung, Alcatel Lucent, Telenor, T-mobile, Instituto de Telecomunicacoes (Portugal), NZ Telecom, and BT. The Institute of Telecomunicacoes was participating only as observer, and they were in contact later to help them build their Open Source Implementation of the IEEE 802.21 Media Independent Handover Framework [107] [108].

This is the summary from the FMCA results:

- All results have been agreed by the 2 participants of each test session.
- All executed test cases run pass, giving 100% of Interoperability.
- NA (Not Applicable):
    - test cases are due to "incompatible" product, i.e. one supporting RDF (Resource Description Framework) format and the other supporting Binary,
    - Or, not all servers support all services.
    - These issues are resolved in real conditions by using MIH Capability Discovery.

Although BT MIIS supported RDF and Binary (TLV, Type Length Value), as well as, MIH Capability Discovery, KT's did not which led to some of the test results to be defined as Not applicable, see Table 6.

Table 6 - FMCA 802.21 IOT results.

		Interoperability		Not Executed		Totals	
Group	Test Id	OK	NO	NA	OT	Run	Results
TC	FMCA Test Case 1	11 (100.0%)	0 (0.0%)	1 (8.3%)	0 (0.0%)	11 (91.7%)	12
	FMCA Test Case 2	12 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	12 (100.0%)	12
	FMCA Test Case 3	9 (100.0%)	0 (0.0%)	3 (25.0%)	0 (0.0%)	9 (75.0%)	12

The following feedback was gathered during the event:

- The TCs (Test Case) available for this Plugtests event provide a good coverage of the procedures involved during MI Handover.

- Further use cases should be considered for the next event, providing additional test cases (for instance multiple PoS, Point of Service).
- Optional test steps shall be moved a an "optional test case", thus splitting current TC into 2 TCs:
    - The mandatory TC including all mandatory steps.
    - The optional TC containing mandatory and optional steps.

Although not mentioned in the reports there was also an experiment conducted by the author of this thesis to sort some of the interoperability issues:

BT was not interested in building a commercial 802.21 structure, which was why when this project was started only the MIIS was considered to be built, although a mock (not so intelligent, not complete) MICS and a MIES were also built to test the MIIS.

In order to be able to use the BT MIIS integrated with other MIH Servers which would have MIIS, MICS and MIES, a MIH proxy was devised. This MIH Proxy could be the first point of attachment for MIH clients, and depending on the configuration can redirect the messages received to one or several MIH servers, see Figure 26. It also can collect the different responses into one and send it to the client acting as an aggregator.

The MIH Proxy utility was proven on the FMCA 802.21 IOT event. 802.21 defined 2 different encodings for MIIS information. As the standard does not have a default encoding, some participants used one way of encoding and others a different one. This meant that some client-server messages couldn't be processed and therefore the communication failed. The MIH Proxy was used to intercept those messages and pass them to servers that were capable of decoding them.

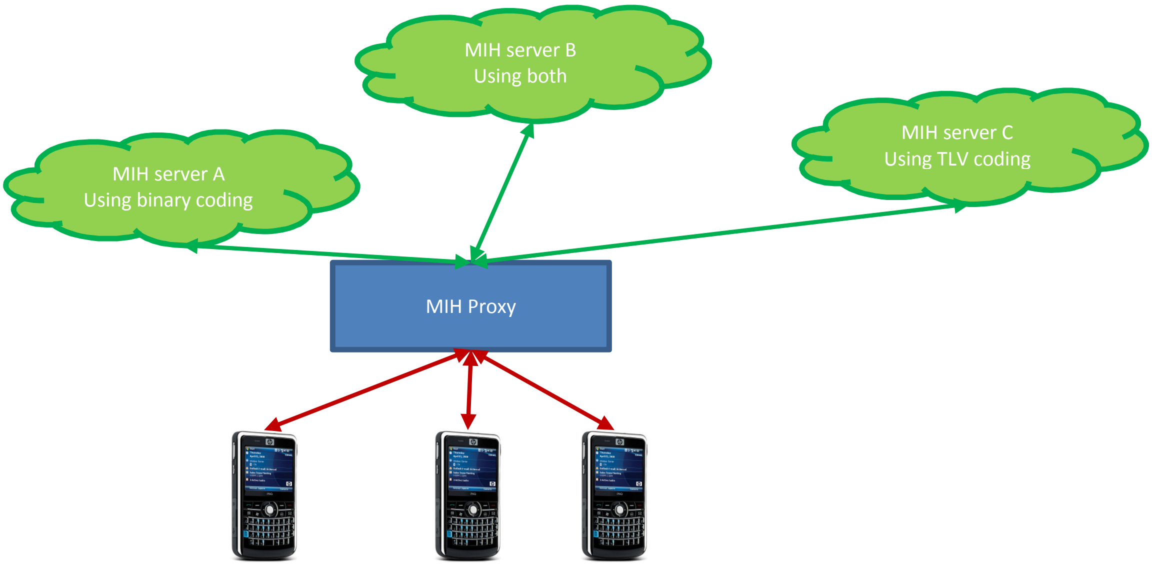


Figure 26 - MIH Proxy diagram.

The idea, is that the MIH proxy allows a higher level of service selection, so it can be configured to use the best MIH services for each user, it can complement the services already offered (mixing/aggregating the results), using MIIS from supplier A and MICS and MIES from supplier B, transcoding between different incompatible formats.

4.2.1. BT MIIS in Mobile World Congress

The BT MIIS was also shown in the MWC (Mobile World Congress) in Barcelona with the support of Interdigital, who provided the client in the device (smartphone and PC, Figure 27) which held the MICS and MECS services [109], IDCM (InterDigital Connection Manager).

In this case, SIP was used to deliver a continuous streaming session from a corresponding Node in the US, see Figure 28, while the MIIS stayed in the UK (it had been previously updated with the available networks in Barcelona). The demonstrator showed a bi-directional handover between 3G (WCDMA, Wideband Code Division Multiple Access) to Wi-Fi (802.11b/g) make-before-break without buffering or bi-cast, which took the data loss from 10 seconds to less than 400ms (worse case measured), see Figure 29.

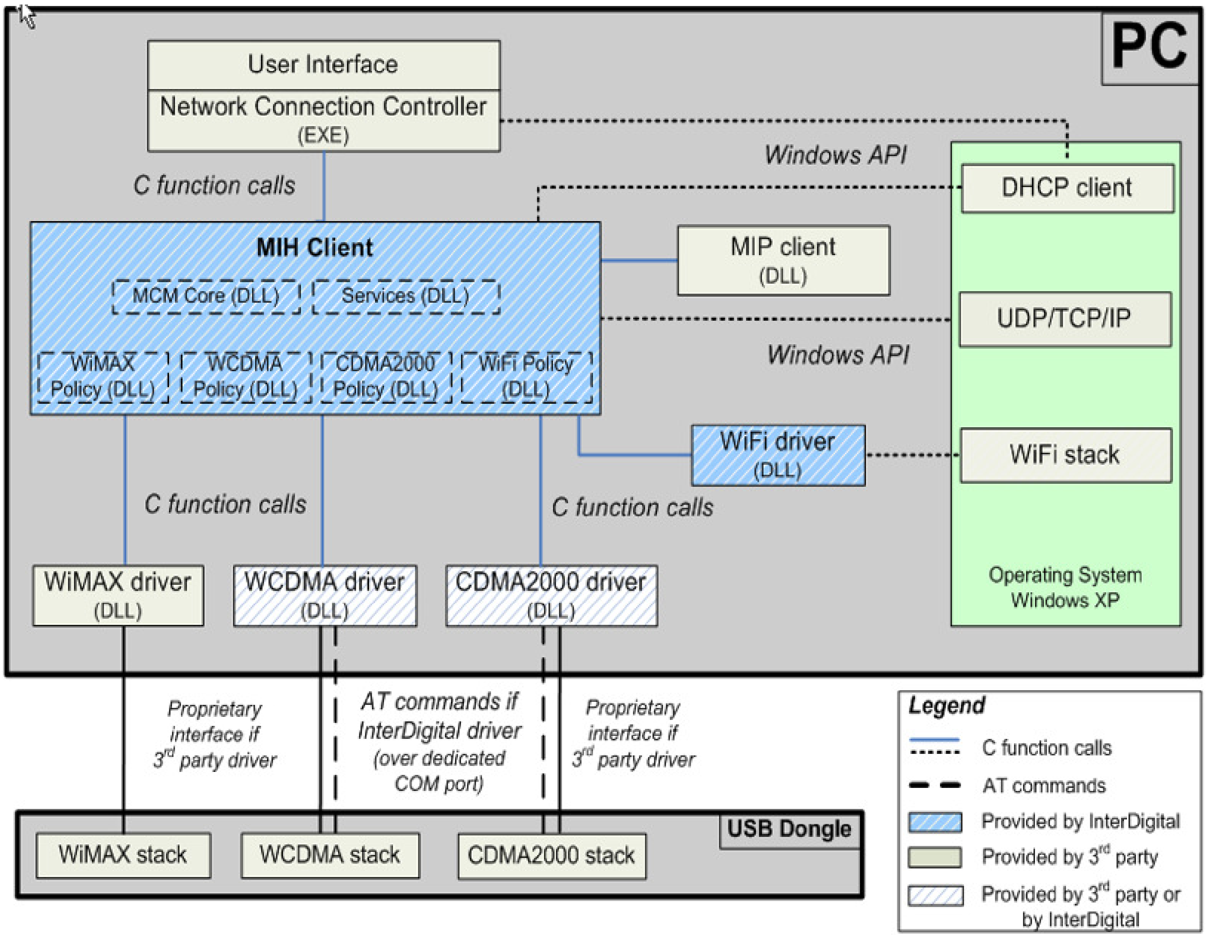


Figure 27 - MIH client representation in a PC (Source: Interdigital 2009).

The handover from 3G to Wi-Fi was triggered by the information received via MIIS and the handover from Wi-Fi to 3G by the degradation of signal sent by the MIES.

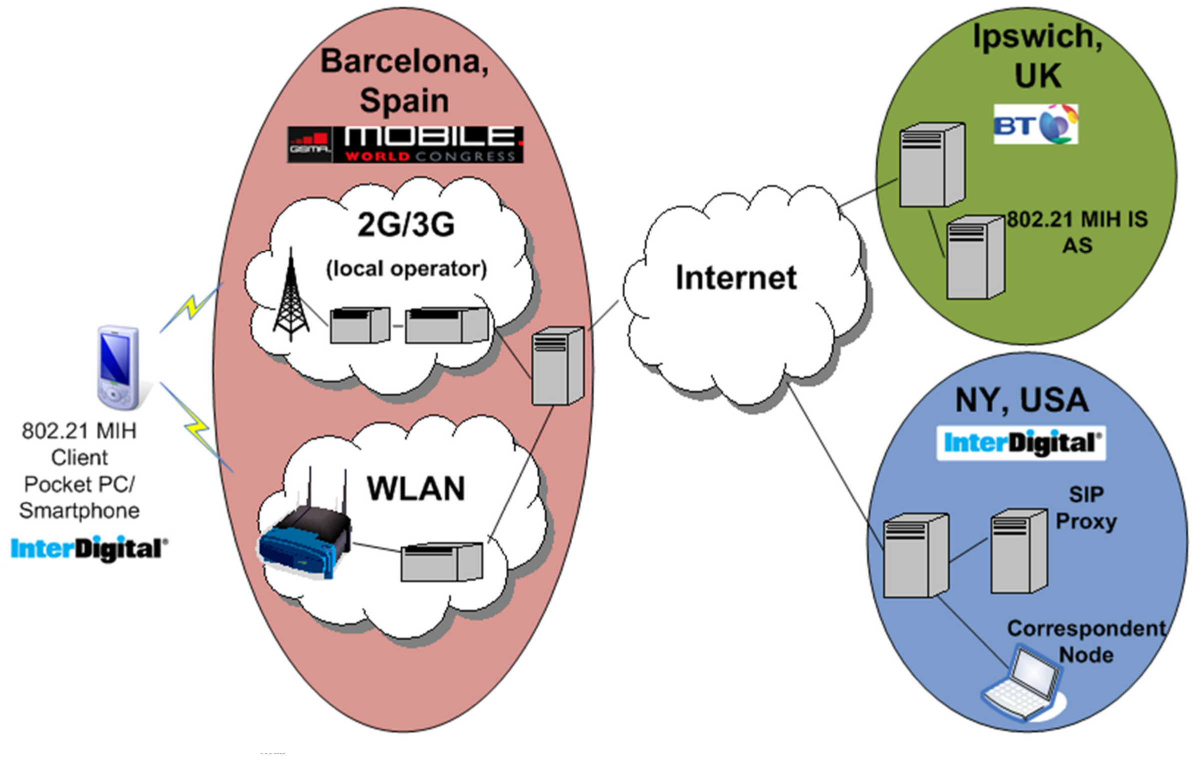


Figure 28 - MIH demo at MWC - Network Architecture.

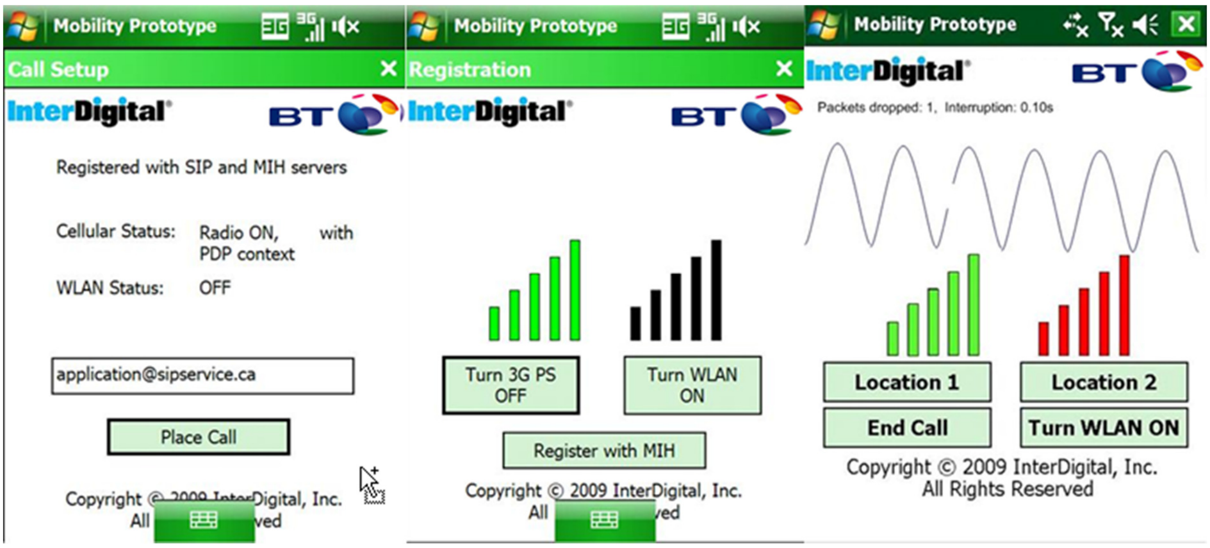


Figure 29 - Different screenshots from the smartphone demonstrator.

This small amount of time to complete a handover allowed also VoIP sessions to handover and therefore, using same architecture of Figure 28 in the MWC 2009 with IDCM we were able to show a VoIP (voice over IP) SIP client (iSIP –intelligent SIP because of its capability to survive an heterogeneous handover) developed by the author in 2008 in C++ for Windows and Windows Mobile 6. The iSIP client coupled with IDCM was able to perform a handover of a SIP VoIP call between 3G and Wi-Fi without disturbance in the user experience, see Figure 30, Figure 31 and Figure 33, to review the call flow and see a screenshot of the laptop version of the client.

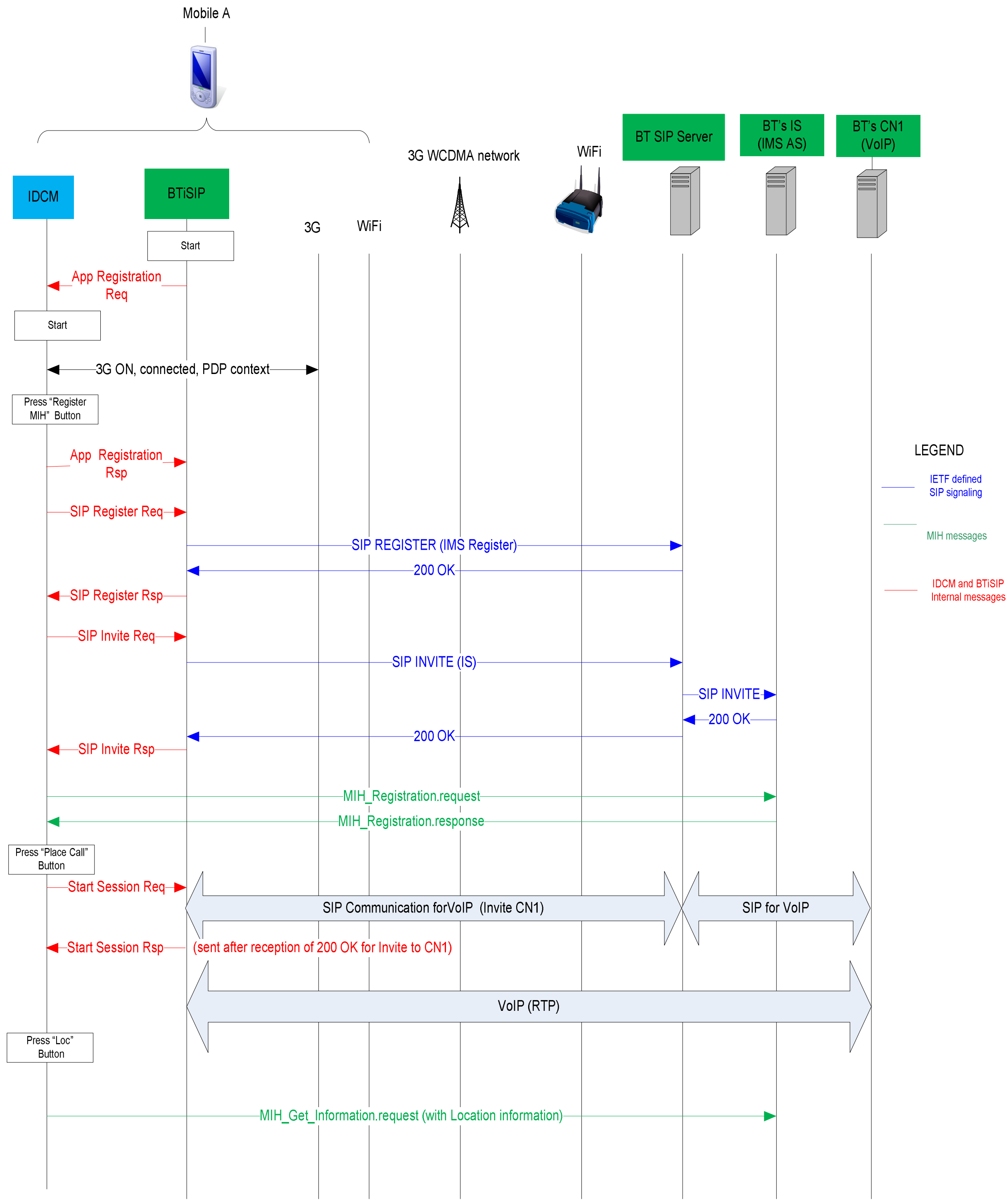


Figure 30 - iSIP call flow 1 of 2.

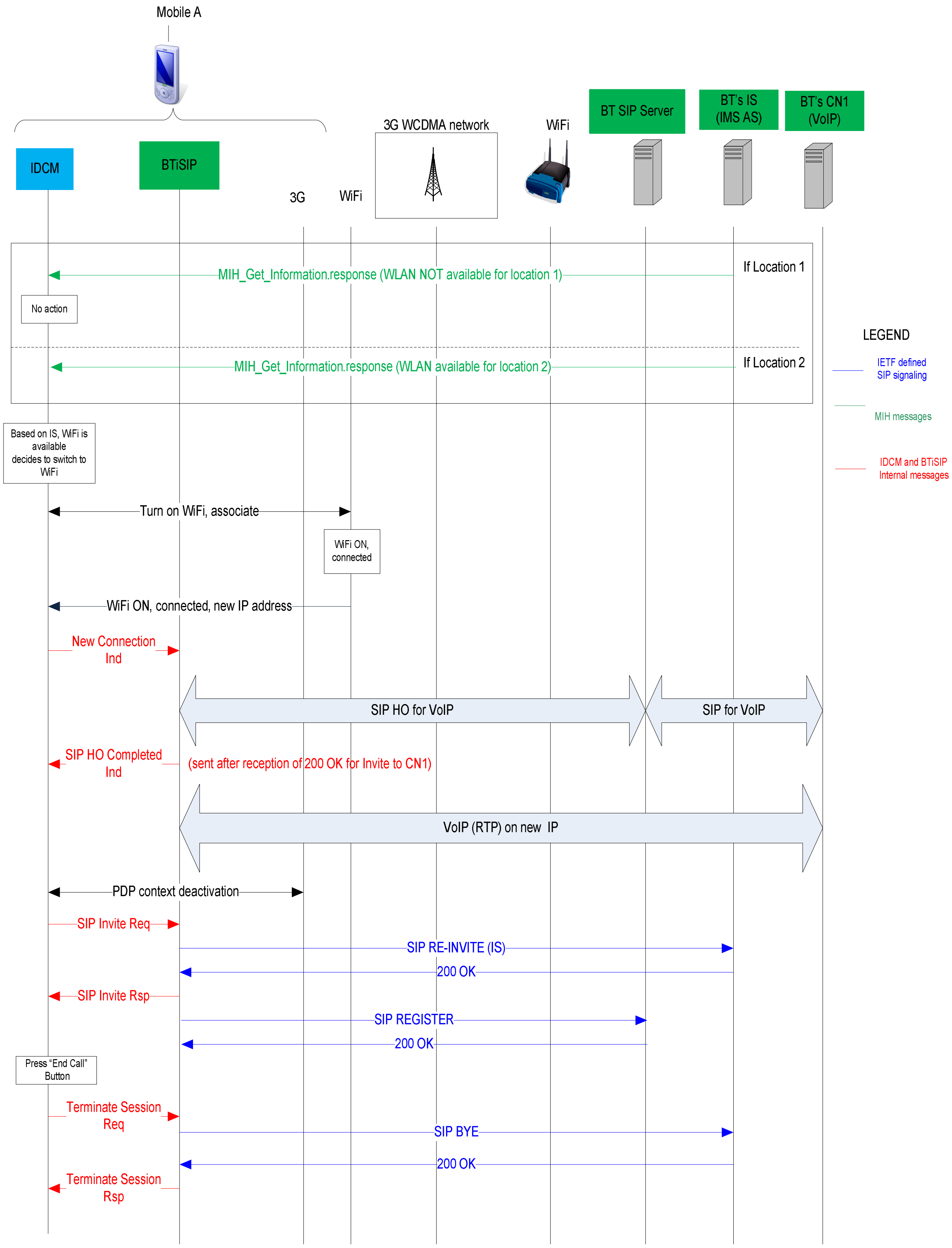


Figure 31 - iSIP call flow 2 of 2.

The client registers the mobile SIP address in a SIP server and also the MIH-ID with the BT MIIS (Media Independent Information Service). After registering the user can make a call and a VOIP session is established via the SIP Server (the VOIP session is set up between another SIP client in a laptop and the SIP client in the mobile device). 802.21 client keeps sending the BT MIIS its current GPS location, so the BT MIIS can return a list of the available networks in that area with information about them (operator, cost, name, channel, etc...). The 802.21 client uses this information to decide if it is needed to do a handover to a different network.

As this was a demonstrator, and therefore controlled and repeatable conditions were desired in a very congested air interface (MWC), the only parameters taken into account for HO between networks were:

- A user preference to use Wi-Fi networks, so it will try to connect and handover sessions to Wi-Fi AP when available. This is quite common as Wi-Fi speeds tend to be higher.
- Wi-Fi signal strength, when it is going down consistently, it probably means the user is moving away from the AP and will lose the connection to the latter and the VOIP call if it is not transferred to another network.
- The available networks in an area discovered via the MIIS.

Other parameters that could have been taken into account but would have made the demonstrator more complicated or less controllable would be:

- Network congestion, a congested network will insert more delay, jitter and less throughput in the transmission and reception.
- Cost of the connection, a more economic conscious subscriber might put a higher weight on much they are charged for using the different networks.
- Device speed, as a device that is moving too fast won’t get any benefits from connecting to a small coverage area network.

Also as the demonstrations would most probably done indoors GPS was turn off and the GPS coordinates were hardcoded to the client which would send them when buttons with the tags “location 1”, “location 2”, were pressed.

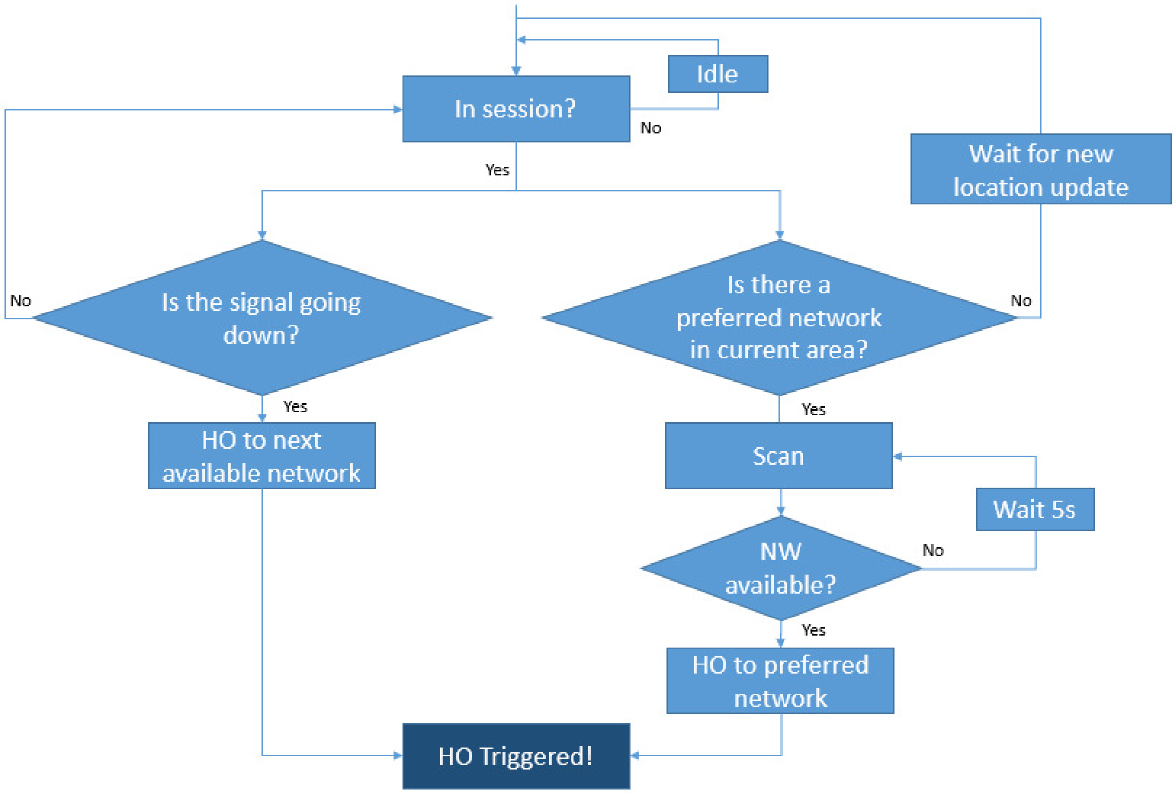


Figure 32 - Demonstrator HO trigger flowchart.

When the 802.21 client decided a HO was required, it checked whether the SIP client was connected, and if so it would turn on the new network radio get an IP, and signal this new IP to the SIP client. The SIP client would then re-REGISTER to the SIP Server and re-INVITE their current VOIP contact, so the packets could be redirected to the new IP. Once the packets are sent and received using only the new radio interface, the SIP client would signal to the 802.21 client that the HO had been completed successfully and this would turn off the old radio interface to save battery.

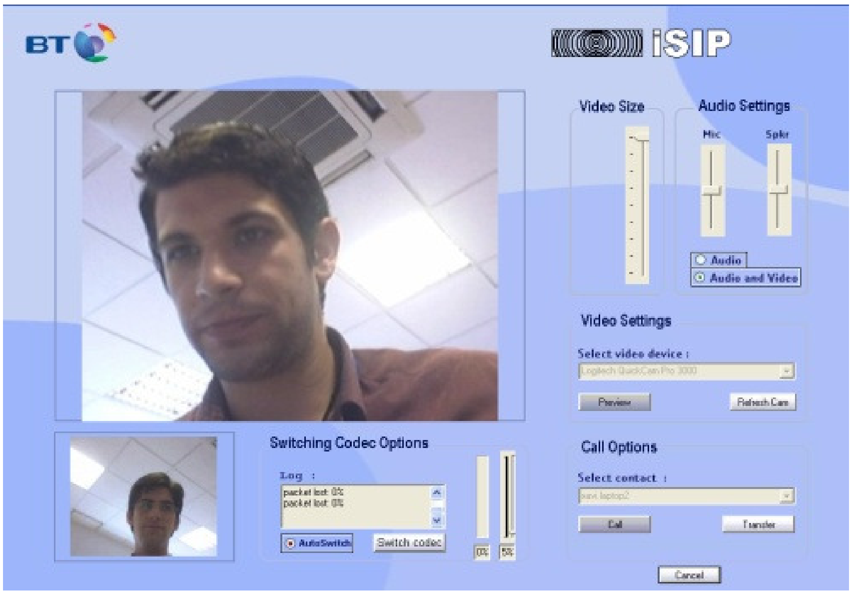


Figure 33 - iSIP laptop version was also able to do videoconferencing and codec switch depending on network conditions.

This equipment and software was used by Olusegun Fatokun, who was under the author's supervision during his placement in BT, in his thesis dissertation to complete his MSc in Telecommunications (UCL) [110]. During his tests he found out that handovers between 3G and Wi-Fi and vice versa took a maximum of 1s with no packets lost (measured from first packet sent or received in new interface to last packet sent or received in old interface). The duration of the handover doesn't affect the QoE as packets are sent and received with both interfaces simultaneously so no packets are lost or delayed, but nevertheless the aim is to make this as small as possible to reduce the amount of time 2 wireless interfaces are active to reduce battery consumption and avoid any issues with out of order packets, as 2 different interfaces can have different delays.

Our own tests of handover times using different applications (VoIP, FTP, and VVoIP) show an improvement of at least 10s and a much lower packet loss over the same tests without the handover triggers of 802.21, see Table 7 - HO duration comparison using iSIPTable 7 and Table 8. Packet loss improvement is especially noticeable in real-time applications as these don't resend undelivered packets.

Table 7 - HO duration comparison using iSIP.

HO duration	VoIP	VVoIP	FTP
Without 802.21 triggers	11.2s	13.3s	10.5s
With 802.21 triggers	0.92s	1.1s	0.89s

Table 8 - Packet loss comparison during HO using iSIP.

Packet loss	VoIP	VVoIP	FTP
Without 802.21 triggers	565 packets	672 packets	0 packets
With 802.21 triggers	0.2 packets	3.1 packets	0 packets

The triggers used in iSIP where added by Intel as an update to the Intel Wi-fi card in the laptop, and functions made available via this driver to make iSIP aware of the HO. This means that if 802.21 became a standard most devices would provide these functions that applications requiring to maintain sessions during HO could use to keep a seamless experience. In the case of SIP sessions, we have explained a working procedure that doesn't require any changes to the standard SIP stack and relies in existing messages, see Figure 30 - iSIP call flow 1 of 2.Figure 30 and Figure 31.

4.2.2. Summary

During 2010 the expectation was that 802.21 and similar technologies would require a Network Connection Manager that would be able to direct and assist devices, especially smartphones, reducing the impact on computing power and battery drainage. But with the recent and expected future improvements in processing power and battery extension, this stopped to be an issue and a connection manager in the device has more chances to respond rapidly enough to changes in the wireless environment.

Therefore, as shown in the tests performed in Section 4.2.1, 802.21 MIIS, or ANDSF, can provide battery savings by only turning on radios that are going to be in use, while also informing devices of the available networks in the area and the conditions these networks are. The impacts of battery saving are well known and the impacts of bad battery management are well understood and shown to lead to subscriber dissatisfaction [111]. The connection manager in the device would have then to make an intelligent decision depending on the current connectivity needs to choose between the available options and using MICS and MIES , or similar, handover the current sessions to the new systems.

What would even improve and make even easier and more seamless the handover between wireless networks would be the usage of a single anchor point (as 3GPP expects with the new EPS) or techniques like PMIPv6 [112] or FPMIPv6 [113] in conjunction with the discovery and management of the wireless networks by 802.21 or ANDSF. The issues that arise from the single anchor point is that all the traffic has to concentrate in that area. Therefore this might increase the cost of core networks for the operator, unless a much cheaper/efficient way of routing core network data is used.

Chapter 5: Authentication & Security Contribution

Mobile networks are generally considered secure, even though some of the very early versions of SIMs and authentication methods have been successfully breached [114]. These breaches have been sorted so in the current versions of 3GPP standards and current networks the level of security still is considered quite high.

On the other hand, public Wi-Fi networks tend to be open and although they provide a secure connection from the access point onwards, the air interface remains unsecure. Simultaneously, these public open Wi-Fi networks often require user authentication to access the internet which requires the user to manually insert settings into the device.

Ideally, we want to use the same authentication methods from 3GPP networks to successfully authenticate against public Wi-Fi access points in a completely secure (encrypted) wireless environment. These methods are tested and proved in Section 4.1.

The required upgrades to support the methods mentioned in Section 4.1 might not be possible in already deployed networks without changing the hardware, for this reason a patented solution is explained in Section 4.2.

The impact of securing instead of a few thousand macrocells to securing potentially millions with the inclusion of small cells and Wi-Fi need to be assessed to avoid disturbance to the core network. This study is done in Section 4.3, and at the same time options to maintain flexibility to manipulate/optimize the delivery of data are investigated (also look in Section 5 for content delivery solutions).

5.1. State of the Art (2011)

With the move to an All-IP network in 4G from the 2G/3G proprietary protocols, it is expected an increase in security issues [115]:

- The open interfaces used on 4G.
- The sharing of infrastructure between operators.
- The high-end end-user devices using open hardware and software platforms.
- The more likely appearance of femtocells in 4G networks also creates the security challenge of having nodes deployed in subscribers' home far from operator control [116].
- The addition of Wi-Fi to the operator's networks.

Apart from the technical reasons, the operators needs to assure their subscribers that their network is securely protected against any kind of threat and their data is safe in the operators' hands.

The signalling and user plane transport in 3GPP networks now runs over IP networks and protocols that are more open and accessible to anyone with physical access and a packet sniffer. This brings a need to provide enhanced protection to traffic running over core network interfaces. To solve this problem 3GPP has developed specifications for how IP based traffic is to be secured between network elements that cross boundaries to untrusted domains.

The protocol stacks in LTE/EPC define a number of interfaces between various nodes such as eNodeB in the radio access domain and MME (Mobility Management Entity), S/P-GW, PCRF, HSS, towards the core network. These specifications define the protocol stacks with the assumption that the network is built within a security domain controlled by one operator using an IP based transport network. The fact that the backhaul implementation and core transport may use public IP media is addressed by security architecture such as NDS/IP as described above. For this reason both IPSec encryption and SeGW functionality are optional in the LTE or EPC architecture, and its deployment depends on operators' deployment strategy.

With the addition of Wi-Fi networks to the mobile operator control, seamless authentication becomes necessary to avoid the need of user interaction and increase usage. Several solutions have been proposed but the lack of standardization makes them unsuitable for commercial operators. With the appearance of 802.1x and the integration work done in 3GPP, see Section 3.6.1, the tools required for seamless handover and authentication into Wi-Fi networks are available.

Nevertheless, there will be a lot of Wi-Fi access points outside the control of the operator and still available to the subscribers. These access points could be a risk for the subscribers and several solutions have been proposed, see Section 5.3.2 for a critical review and comparison to the authors solution.

5.2. 802.1x Integration into BT Wi-Fi

Before the start of this study, 802.1x had not yet been implemented or tested in the real network by BT, even though BT research had been informing the business about the benefits of using 802.1x (802.1x-2010, superseded by 802.1x-2013 [117]) to provide seamless authentication and optional point to point encryption into the BT Wi-Fi access points.

Because of this, it was decided a small placement with the BTOZ (BT OpenZone) design team would kick-start the integration of 802.1x into the BT Wi-Fi network and at the same time help understanding how a network with a high number of small cells (in this case Wi-Fi) could be deployed and the difficulties they had found.

To start, a way of bypassing the core security of BTOZ for 802.1x requests had to be found (to get any IP connectivity the user had to authenticate), so they could then request to authenticate with the authenticator (Cisco ISG, Intelligent Services Gateway, Farms) which would forward then a radius request directly towards the BTOZ AAA (Authentication Authorization and Accounting) server. This server then could, if required, forward the authentication to another external AAA server, see Figure 34. This last point was especially interesting, as it opened the doors to allow seamless authentication that BT Wi-Fi could sell to other mobile operators while keeping the credentials still in the operators' control and without BT being able to intercept. This was later offered and incorporated to O2 and Vodafone for their IOS products to authenticate into BTOZ [118].

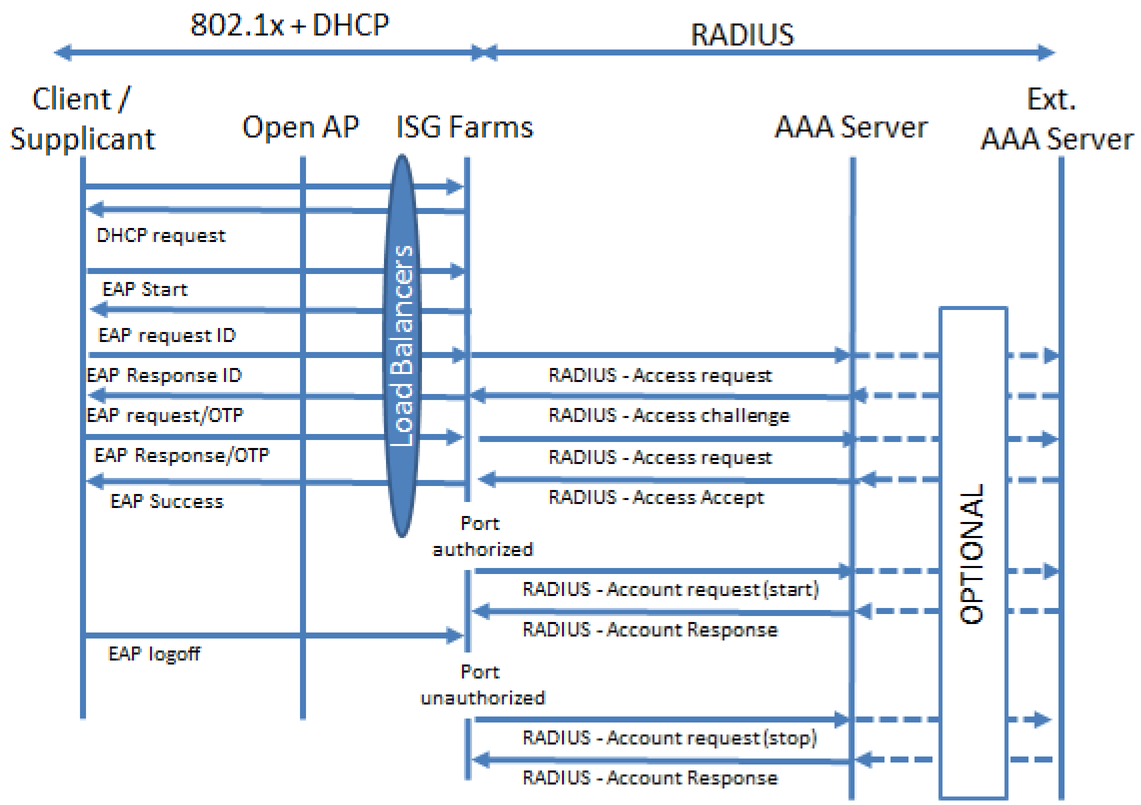


Figure 34 - 802.1x authentication process in BT OpenZone.

To achieve this first objective, focus was put on the BTOZ load balancers and in the type of authentication requests used by 802.1x. A filter was created that allowed 802.1x authentication requests to reach further into the network up to the ISG (BT core controller/authenticator). EAP-TTLS (Tunnelled Transport Layer Security), using a certificate installed in the device, was being used to authenticate but any EAP-like authentication would had been able to reach the AAA server. The load balancers had to be reprogramed to recognize the 802.1x requests and also exceptions added in the DHCP and DNS (Domain Name Server) servers so the 802.1x clients could find the AAA server with the initial DHCP query, Figure 35.

When the authentication was successful it was used as a demonstrator of the 802.1x integration on BTOZ for internal and external customers, and it became the first implementation of 802.1x in the live BTOZ network.

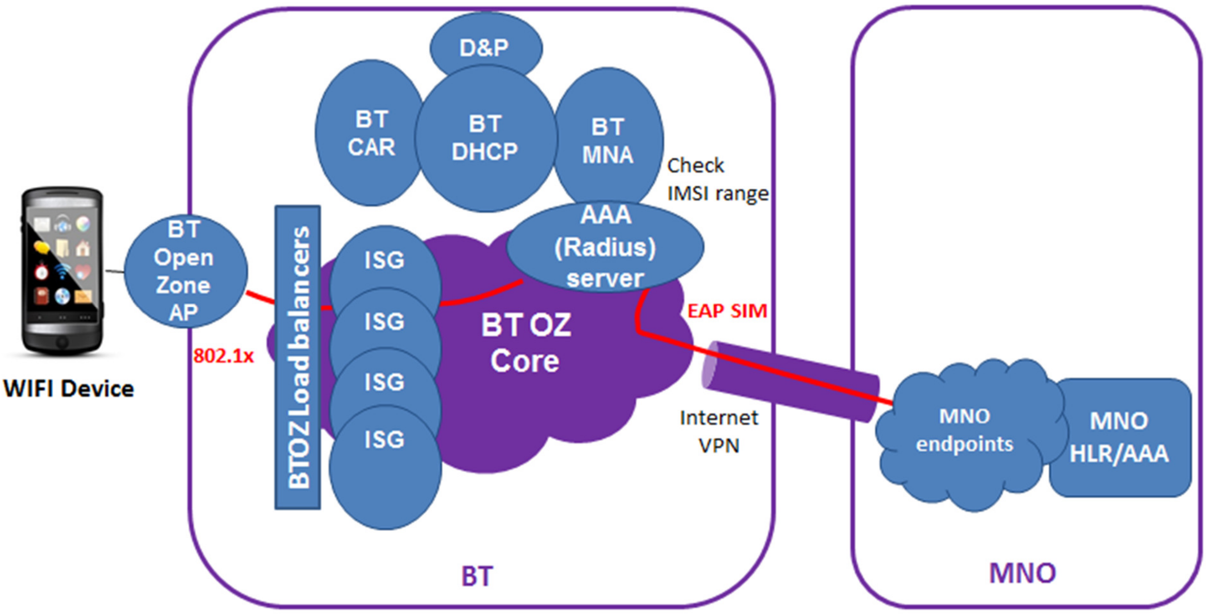


Figure 35 - BTOZ 802.1x authentication using EAP-SIM with integration to a 3rd party MNO HLR (Home Location Register)/AAA.

After this initial success, a solution had to be designed that would allow the traffic to flow via the core security of BTOZ so all the current statistics and policies remained intact.

Two solutions were proposed that involved small changes in different parts of the structure.

1. First solution was based in the demonstrator filter, this clearly meant that each device when authenticating would require to use the DHCP server to find the AAA IP address.
2. The second solution was to modify the AP to segregate 802.1x traffic to a different set of Load balancers that would allow all traffic to go to the AAA. The modification on the AP was not difficult to make as the setting to send 802.1x data via a different path already existed within the software.

These solutions were analysed, and, although they were verified as possible solutions, both meant the DHCP server of BTOZ would be overused, and that could mean a degraded service for all customers.

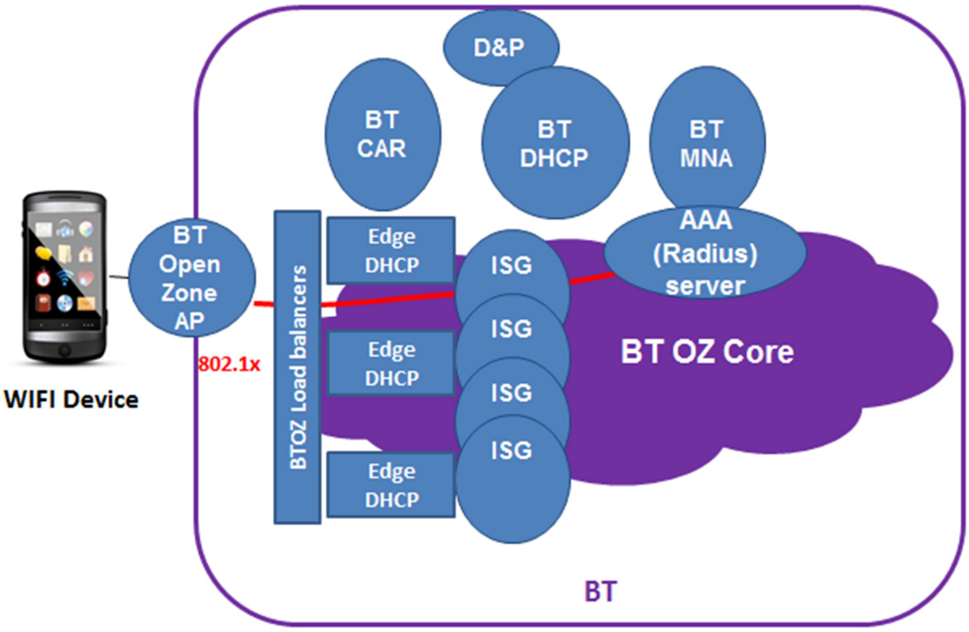


Figure 36 - Final BTOZ design with edge DHCP to take load of main DHCP server.

After some thought, it was decided that if the problem was the DHCP usage, a smaller DHCP closer to the edge of the network for 802.1x traffic only could be added and thus absorb the extra load. At the same time this solved the increased load on the central BT DHCP due to BTOZ success, so it was already a change that had been thought about and the requirement for 802.1x only made the change to happen earlier.

This was at the end implemented and deployed and it is part of today's current solution, Figure 36. On average the 802.1x authentication in BTOZ takes 3.7s most of the time is taken by the time it takes the AAA/Radius server to reply while the authentication keys are checked, but at peak times when many requests are sent simultaneously the average response time can go up to 27s. This is not ideal, and it shows that the AAA capacity should be expanded to cope with the load, on the other hand, the edge DHCPs are coping well with traffic (average dhcp reply is 28ms in Baynard Node and 19ms in Eldon Node) and their responses even at peak times are under the 100ms.

While doing this integration, a great deal of detail about the architecture of BTOZ and its complexity was learnt. The main issue with BTOZ was that it had been growing organically depending on the needs of the different sites where it had been installed; no one expected in its beginnings that it would be so successful (in 2013 BT Wi-Fi has already over 5million access points to manage and 13 petabytes of data per year [119]).

5.3.Point of Access Authentication – Patent Filed April 2010

802.1x is a robust solution to provide a secure authentication in a public open Wi-Fi environment, but there are lots of public open Wi-Fi networks that are not going to change their infrastructure in the short term to allow this extra level of seamlessness and security.

For this reason, a way to implement a secure way of connecting to any other wireless solution avoiding security pit-holes like man-in-the-middle attack was looked for. We looked for a solution in which the public/private keys could be exchanged in a secure way using the mobile network before even connecting with the Wi-fi AP, this way no contact would have been made with the Malicious AP and any communication with it would be already encrypted and protected.

Thinking in the future scenario where there will be several wireless networks overlapping each other, the possibility of using the current connected network to authenticate to the newly discovered one seemed possible. To allow this solution, information about all the possible networks in a specific location was desired, the author had also been involved in the first plugfest/IOT of 802.21 aka MIH [120], one of its components being the MIIS of which one of the earliest versions had been developed, and therefore it was known it held a lot of the information needed to enable verification and authentication of an unknown access point without exchanging any subscriber information insecurely.

The basis of the solution was that mobile networks are inherently secure due to their usage of the credentials securely stored on the SIM card (UICC). Old SIMs used DES (56 bits) as encryption mechanism and this can be cracked with an average current computer within minutes, but current SIMs use 3DES (112 bits) and AES (128/256 bits) which would take even current supercomputers trillions of years to crack [121] [122].

Therefore using that existing authenticated connection it was possible to query an MIIS that would hold all the registered available networks[1], verify the location, MAC, and secure keys of the access point (AP) and then with this information try to authenticate in a secure way. Once you authenticated to one AP you could reuse this verified secure connection to authenticate into other nearby APs.

---

[1] There had been discussions on who would be in charge of keeping an up-to-date database with all the wireless information of the MIIS. Several scenarios have been discussed in the standards meetings, for example where a national database could be offered as a service to different operators. Or where each operator would have their own service offered only to their subscribers and where they would add only networks they had agreements with.

This solution of reusing MIIS functionality to improve security on public open wireless networks resulted in the patent described in the next Sections [7].

5.3.1. Patent Summary

This patent was filed on the 30th March 2011 as "METHOD AND SYSTEM FOR AUTHENTICATING A POINT OF ACCESS" [7] with Xavier Jover Segura and Fadi El-Moussa as inventors.

The patent tries to solve the issue of rogue access points within the existing infrastructure. In order to prevent this threat a method and system is proposed that verifies that an access point is genuine and not rogue before setting up a connection between the access point and a wireless device. The authentication is based on comparing an identifier of the wireless device obtained from an authentication server in the wired network to an identifier of a wireless device obtained directly from the wireless device. A comparator in an information server receives the two sets of data and compares the two identifiers and if they match the access point is verified as genuine.

The following steps, see Figure 37 and Figure 39, give an idea of a possible implementation of the patent:

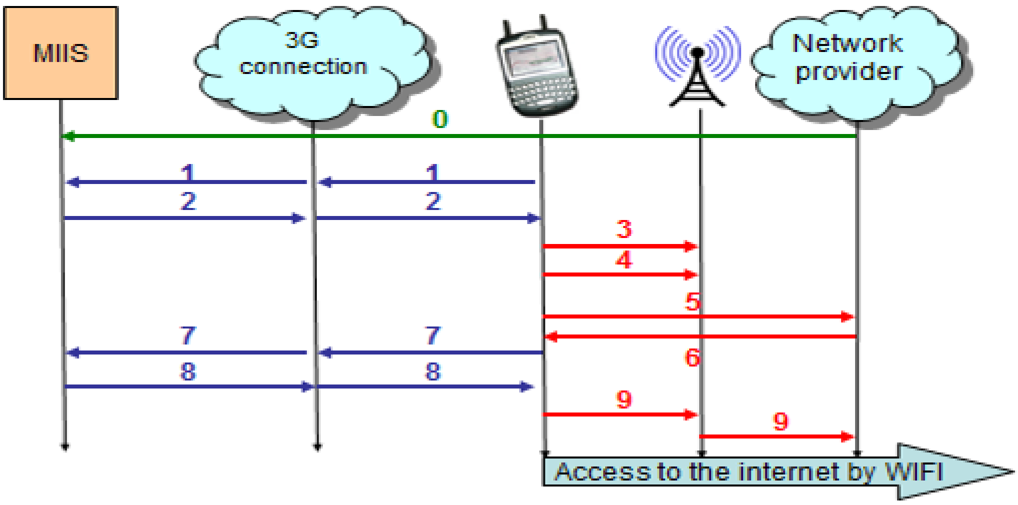


Figure 37 - Step by step description of one of the patent possible implementations.

- **Step 0:** A Wi-Fi network provider creates a relationship with the MIIS service owner to add their APs information to the database, this can be information like location, bandwidth, MAC of wireless interfaces, SSIDs, etc.
- **Step 1:** A device already connected and authenticated to the mobile network requests information about surrounding wireless APs using its own location.

- **Step 2:** The MIIS responds with info about a suitable network it can connect to with information about the AP such as SSID, MAC address, Network provider, Cost, Bandwidth, etc.
- **Step 3:** With this information the connection manager can choose which AP to connect to, based on the user's requirements.
- **Step 4:** Thereafter, the connection manager at the wireless device will connect to the selected access point and, as configured by the installed software program, it will request an authentication message from the Network Provider (NP). Preferably, the current 802.11 association request is used also as the request for an authentication message. 802.11 is the Wi-Fi standard so this is a packet that has to be sent anyway, and already contains the device and the AP MAC addresses. This packet is then encapsulated in an IP packet by the access point and sent directly to the NP controller.
- **Step 5:** Upon receiving the request the NP controller is configured to create the following authentication message, which is sent as an add-on in the 802.11 association response to the access point which then forwards the message to the wireless device, see Figure 38 below:

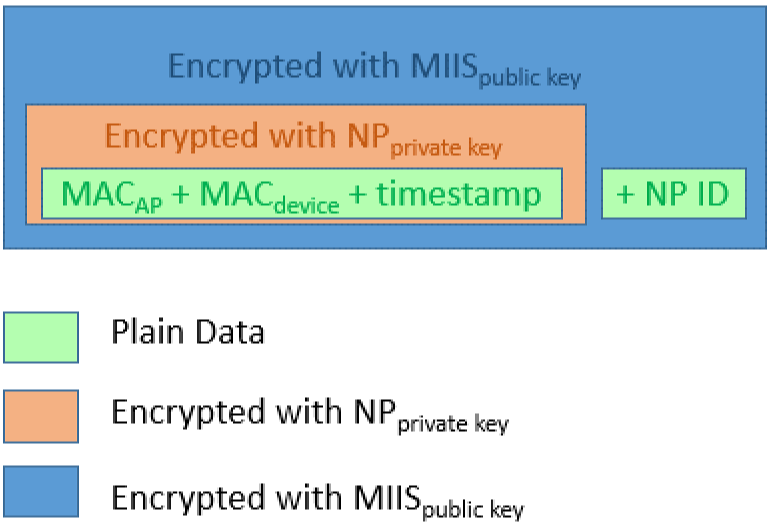


Figure 38 - Patent authentication message.

The authentication message consists of the following:
MAC of the AP (MAC_{AP}), MAC of the wireless device (MAC_{device}) requesting access to the Internet and the time of request (time) all encrypted with the Network Provider private key (NPpr), the MIIS has the NP public key already stored. Encrypting with the private key serves as a signature. Various signature algorithms could be used (e.g. DSA (Digital Signature Algorithm), or where symmetric encryption is used between the NP controller and the MIIS; Message Authentication could be used. In either case, encryption of the signature is not required to assure the authenticity and integrity of

the message on arrival at the MIIS. The entire previous message is further encrypted with the MIIS public key (MIISpu) which has been shared with the network provider previously.

- **Step 6:** The connection manager will acknowledge the response and is configured by the software program to send the authentication message to the MIIS to authenticate using a previously authenticated network such as 3G.
- **Step 7:** The MIIS will decrypt the received message using its private key, and then read the NP ID to locate the appropriate public key to decrypt the rest of the message (MAC_{AP}+MAC_{device}+time). Once the MIIS decrypts the message using the NP public key, then it will validate the message time and compare the decrypted MAC address of the access point to stored access point MAC addresses in the database, as well as comparing the decrypted MAC address of the wireless device with the MAC address of the device that forwarded the authentication message to the information server to make sure that the access point as well as the wireless device forwarding the message are genuine and not rogue. If, for example the authentication message is forwarded on an already authenticated Wi-Fi network, instead of a 3G network, the MAC address of the device sending the message can be obtained from the 802.11 header. If a 3G network is used another identifier, for example the telephone number for the device, can be extracted and the MAC address for the device can be looked up in database in the server, which database stores phone numbers and corresponding MAC addresses for devices registered for the authentication service.
- **Step 8:** Successful or unsuccessful verification result is then sent back to the connection manager at the wireless device with the login credentials (which can be one use only if so desired).
- **Step 9:** The connection manager will use the login credentials to access the network of the network provider via the selected and authenticated access point. Hence, a user does not need to remember his credentials for each network provider but can login automatically to the selected network knowing that the access point is authenticated and thus be sure he is not connecting to a rogue access point. All the login credentials are encrypted and unavailable to the user; only the connection manager in the device is able to decrypt the login credentials thus preventing users from sharing credentials.

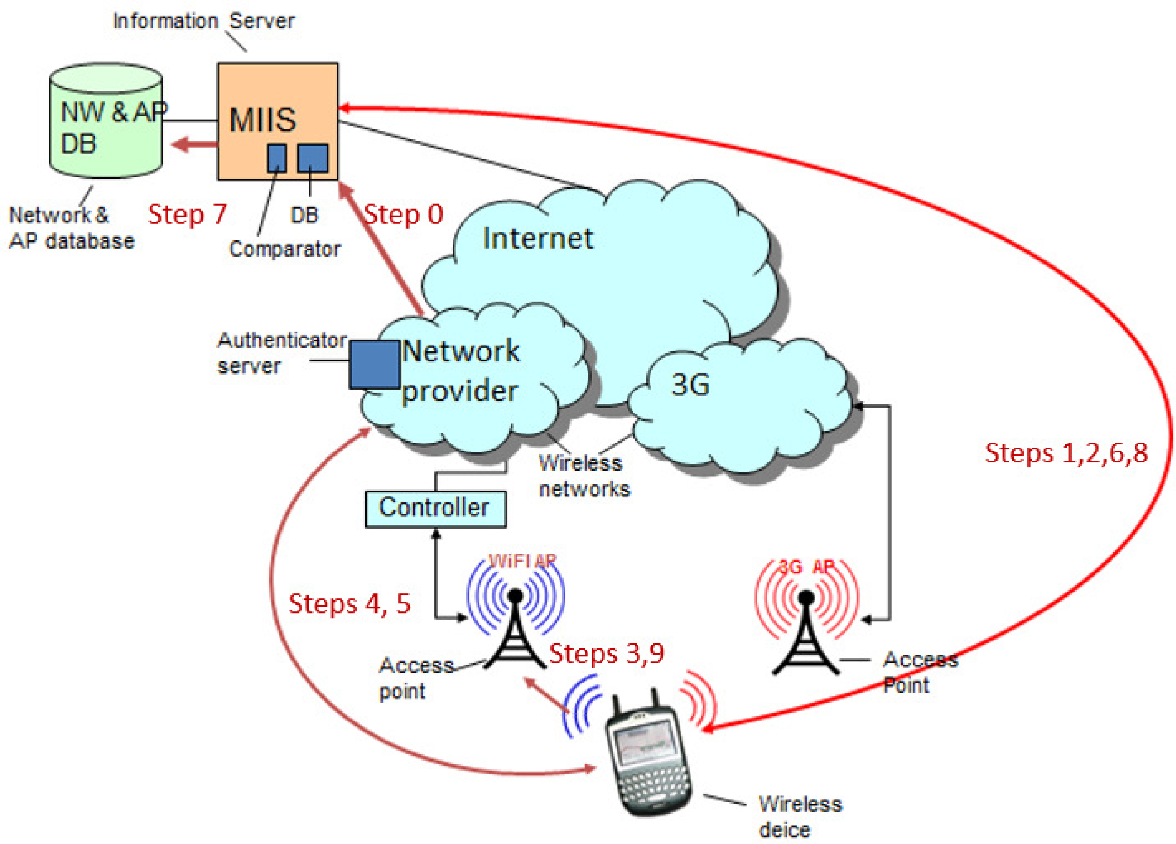


Figure 39 - Network diagram of possible patent implementation.

5.3.2. Previous Solutions

Previous solutions and issues with them:

- A method for dealing with rogue access points is described in the patent application **WO2008/095291** [123]. In some of its solutions the combination of a wireless network's SSID and the AP's MAC address (Media Access Control address) is verified when a wireless device first connects to an access point. The administrator of the WLAN provides registration information regarding itself, including the desired SSIDs to a central server. The central server receives the registration information and connects with a database registry containing all registered SSIDs. A check is performed to ensure that the desired SSID has not already been registered. If the desired SSID has not been registered, the central server creates an association between the SSID and each AP MAC address of the WLAN. This association is stored in the database registry. The central server then transmits the registration information to a certificate authority. The certificate authority performs validation of the registration information and if the validation passes, the certificate authority issues for each access point within the WLAN digital certificates associating the AP MAC address with the SSID of WLAN. Such a digital certificate is transmitted to each access point of the WLAN.

Once the wireless device is connected to the access point of the WLAN, the access point of the WLAN transmits the digital certificate to the wireless device. The wireless device connects to the central server through the access point and submits the certificate and SSID to the central server. The central server authenticates the digital certificate and verifies that the purported network identifier is indeed associated with the WLAN to which the AP with this MAC address belongs. This ensures that the WLAN to which the wireless device is connecting to is the one to which the wireless device is intending to connect.

The known method remains vulnerable to a so-called man-in-the middle-attack; the certificate can be sniffed and copied and used by rogue access points. The application suggests the use of traceroute information to prevent sniffing; however, tracerouting is not suitable in an IP network since packets can be routed over many different routes between the same endpoints and further, nothing prevents a rogue access point from spoofing also the traceroute packets. This is avoided by the authors patent by adding a timestamp to the authentication message, and the MAC of the device, making the authentication message unique and time constrained for the intended subscriber. Both the MAC of the device and the timestamp are encrypted so can't be changed or tampered with.

- **US20040198220** [124] discloses another system for securely accessing a wireless network. The system includes a security server that subscribes to messages from an SNMP trap on the access point. When a mobile unit associates with that access point, the trap sends a message indicating the association information. A roaming control client on the mobile device polls the security server, which verifies (or not) that it has received the message for that association.

  A disadvantage with this system is that since the wireless device polls the security server via the unauthenticated access point it is likely that the device will have exchanged several messages, likely including sensitive data, with a possibly rogue access point before even realising that it is a fake access point.

- **EP1542406** [125] discloses an impersonation detection system for a wireless node. The node comprises an intrusion detection module for correlating original data frames, transmitted directly by the wireless node over a secure link to the intrusion detection module, with incoming data frames received over the air interface. If the wireless node is inactive but the intrusion detection module receives traffic that indicates that the monitored node is the originator, then this would be a sign of suspect behaviour since correlation of the data sets would not result in an empty data set.

This is a fairly complicated system in which the intrusion detection module constantly has to monitor the channels allocated to the node using an antenna in order to compare frames. Another disadvantage is that the wireless node has to be connected to the intrusion detection module over the secure link and if this link fails for some reason the system does not work. It is also a disadvantage that the node needs to have two connections running most of the time. The authors patent avoids these over complications by relaying in standard procedures already available or soon to come with the exception of the connection manager functionality in the device.

5.4.Security in LTE Networks, Deployment Options and Tests

From the standards perspective, SeGWs (Security Gateways) are entities on the borders of the IP security domains used for securing native IP based protocols, see Figure 40. The SeGWs are defined to handle communication over the Za interface, which is located between SeGWs from different IP security domains protecting the traffic with IPSec. In summary, the specifications require:

- All NDS/IP (Network Domain Security IP) traffic is passed through a SeGW before entering or leaving the security domain.
- Each SeGW is defined to handle IP traffic in or out of the security domain towards a well-defined set of reachable IP security domains.
- Each security domain can have one or more SeGWs, depending on:
    - The need to differentiate between externally reachable destinations. In case that different SeGWs are used to reach different external destinations.
    - The need to balance traffic load. In case the load traffic is high enough to require more than 1 instance.
    - And the need to avoid single points of failure. As all traffic needs to be processed by the SeGWs these become a single point of failure and operators tend to duplicate them both in the same location and in a second geographical location.

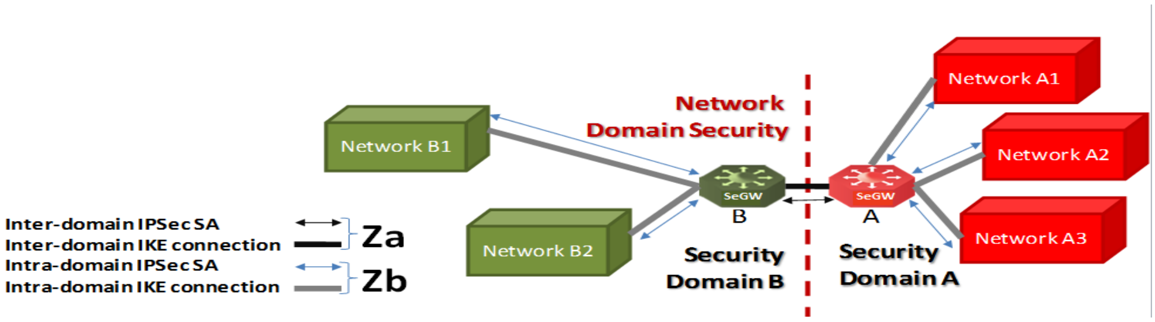


Figure 40 - SeGW standard use to protect different network domains (Source: Stoke Inc.).

IPsec is a network layer security protocol with the following components:

- **Two security protocols, AH (Authentication Header) and ESP (Encapsulating Security Payload).** AH can provide integrity protection for packet headers and data, but it cannot encrypt them. ESP can provide encryption and integrity protection for packets, but it cannot protect the outermost IP header, as AH can. For a VPN (Virtual Private Network), which requires confidential communications, ESP is usually chosen.
- **IKE (Internet Key Exchange) protocol.** IPsec uses IKE to negotiate IPsec connection settings; authenticate endpoints to each other; define the security parameters of IPsec-protected connections; negotiate secret keys; and manage, update, and delete IPsec-protected communication channels.
- **IPComp (IP Payload Compression Protocol).** Optionally, IPsec can use IPComp to compress packet payloads before encrypting them.

There are mainly two types of SeGW:

- **Integrated** with other equipment, usually software based, which in some cases when terminating many IPsec tunnels it has been said that can reduce the performance of the equipment for its original use (MME or SGW in the EPC). With performance degradation of 80% to 90% when compared to the same equipment just running plain IP [126].
- **Standalone**, usually hardware based, with more capacity in terms of number of IPSec termination and processing of encryption/decryption algorithms, and no effect on the performance of existing equipment.

'Open IP Network' from eNB (enhanced Node B) towards core network makes EPC nodes susceptible to attack and intrusion. Of special relevance to EPS (Evolved Packet System) and E-UTRAN (Evolved Universal Terrestrial Radio Access Network) is the S1-U interface between EPC and the LTE RAN. This interface needs to be fully protected through implementation since the user plane data protection would otherwise be terminated in the eNodeB, potentially exposing sensitive data as it passes between the eNodeB and the EPC core. This could allow unauthorised access or DoS (Denial of Service) attacks on operator equipment and services and subscriber data can be intercepted, permitting malicious theft of service or sensitive information or corruption of user data.

Also by using the SeGW as the switching path between eNodeBs, it alleviates network resources both at the eNodeB and the EPC. 3GPP documents an X2 interface [127] for inter-eNodeB mobility, therefore the SeGW becomes an X2 switch, removing the overhead of maintaining a list of security associations from the eNodeBs and reducing mobility signalling on the EPC nodes, as performed by the X2 interface among eNBs. It could be especially crucial on small cell sites where 100s of mobility events will occur, due to the proximity between cells and their small size, handovers will be more frequent.

As an initial deployment model, MNOs may be tempted to implement IPSec by reusing built-in SeGW functionality available within their eNodeB, SGW and MME nodes, as shown in the diagram below, Figure 41.

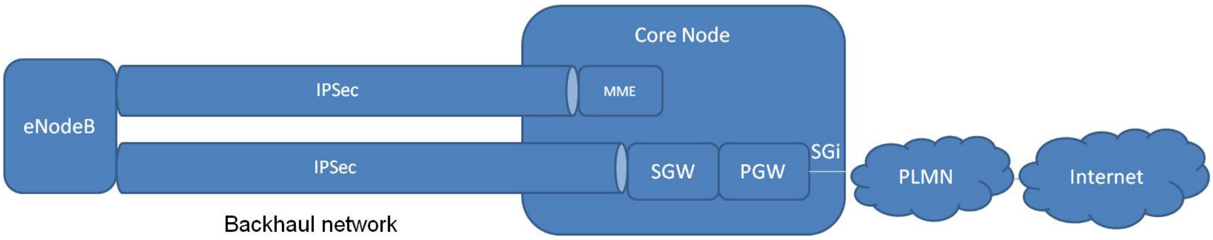


Figure 41 - Basic implementation – built-in SeGWs (in MME and SGW).

In this deployment model, the only point of content insertion or optimisation is the SGi reference point in the MNO's core network, ruling out the possibility of applying any level of intelligence or value-added services to traffic over the backhaul network.

5.4.1. Optimising Core Network Performance – Stand-Alone SeGW Functions

There is an expectation that, the growing demand for data traffic coupled with the need to deploy a large number of LTE small cells (e.g. for indoor coverage) will stretch the capacity of the core network elements to support the data throughput (on the SGW) as well as the number IPSec tunnels required (on the SGW and MME). We expect this to result in a need to deploy stand-alone SeGW components in the MNOs networks which can:

- Reduce throughput over the SGW by removing the traffic overhead introduced by IPSec tunnels (estimated to be between 15% and 20% on average – being analysed in phase 2 of the SeGW tests in Section 5.4.4.
- Reduce the processing load required on both the MME and the SGW by removing the need to terminate a large number of IPSec tunnels – this is especially beneficial on the MME, which is a heavily centralised function having to handle a large number of eNodeBs in the network.

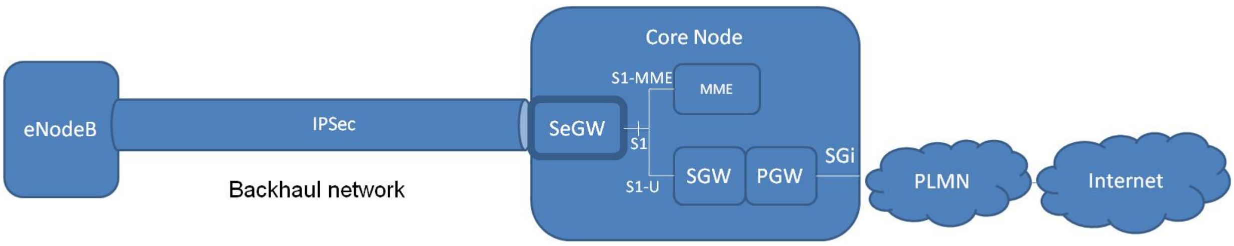


Figure 42 - Stand-alone SeGW located in the core.

In this deployment model, Figure 42, content can only be inserted at the SGi reference point, just as in the basic architecture, whereas additional content optimisation or intelligence may be deployed before the SGW, i.e. on the S1-reference point when it enters the core node. Having said that, any content optimisation and/or traffic intelligence applied at that point presents little or no advantage compared to applying the same techniques on SGi, other than cost savings on SGW/PGW capacity that is likely to be offset by the cost of introducing and maintaining the optimisation solution itself.

5.4.2. Optimising Backhaul Capacity and QoE– Distributed SeGW Functions

It is foreseen that there are three main reasons for MNOs to selectively deploy some of their SeGWs closer to the edge of their networks:

- Reduce costs by:
    - Reducing throughput over the backhaul network, by terminating IPSec tunnels closer to the edge of the network thus removing the traffic overhead introduced by IPSec – this is provided that MNOs trust the level of security provided by the backhaul network, even if provided by a third party (Figure 43).

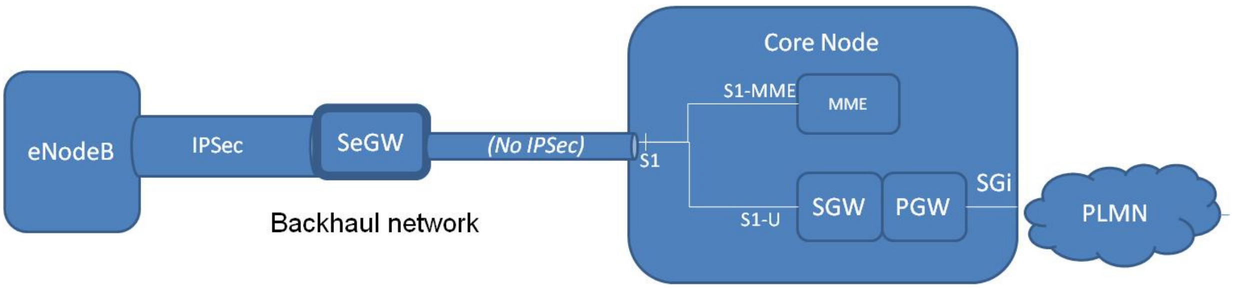


Figure 43 - Distributed SeGWs - traffic overhead reduction over the backhaul.

    - Enabling content insertion, IP offload and content delivery optimisation techniques to be applied at the edge of the network by terminating IPSec tunnels on the most optimal points of traffic aggregation (Figure 44 and Figure 45). These points would vary depending on the network architecture of the operator, where their Content Delivery Nodes where located and where their points to pair towards the internet are.

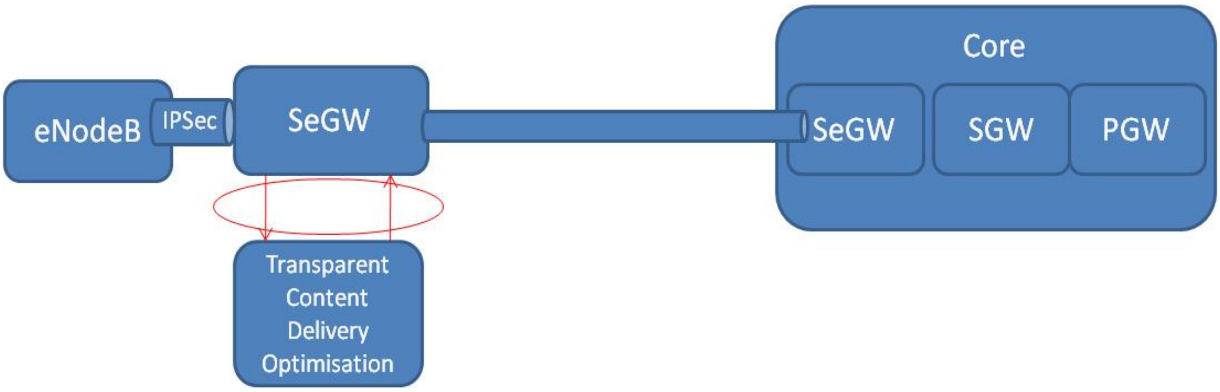


Figure 44 - Distributed SeGWs - content delivery optimisation at the edge.

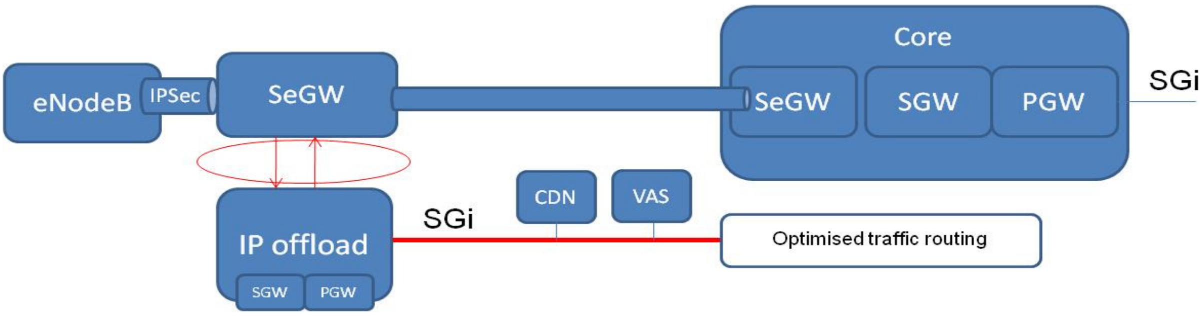


Figure 45 - Distributed SeGWs, IP offload, content insertion and other Value-add services at the edge.

- Improve the quality of experience by:
  - Enabling faster inter-eNodeB handover using X2. The assumption here is that, if X2 gets implemented between adjacent eNodeBs, IPSec encryption would have a negative impact eNodeB performance because of the high computational load that IPSec requires, this would be even more obvious in small cell deployments where each eNodeB is likely to have to communicate with a large number of (10s of) adjacent eNodeBs using X2 (Figure 46) and where the eNodeBs would have less computational power (smaller devices with less power and with costs constraints).

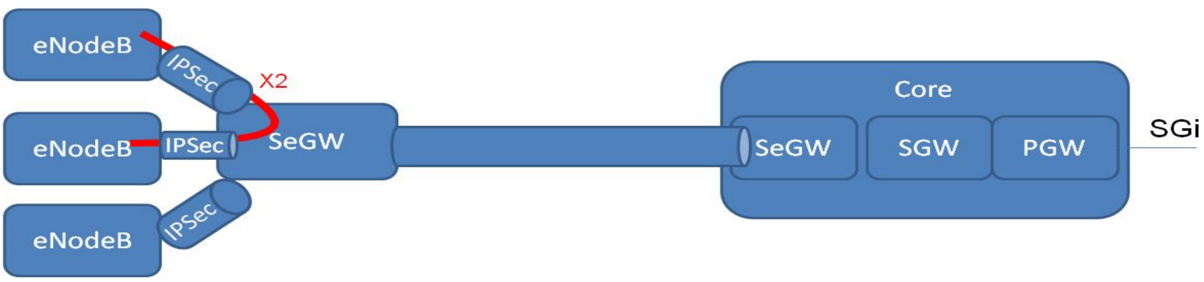


Figure 46 - Distributed SeGWs, enabling X2-based handover whilst minimising the impact on eNodeB performance.

- Enabling content injection and/or optimisation at the edge of the network, as already depicted in Figure 44 and Figure 45 above, which can improve the experience of the end user when consuming content (video or others).

It is this last deployment model, where stand-alone SeGW functionality can be implemented in the backhaul network that presents an opportunity for BT (or any other wholesale backhaul operator) to provide services to the MNOs beyond pure transport. BT could host and manage SeGWs at selected points of traffic aggregation, in the exchanges for example, where BT may cost-effectively deploy shared platforms to support content caching and delivery, optimisation, optimal routing and other value-added services to a number of MNOs.

5.4.3. Phase 1 Testing Scenarios

The following test scenarios and results are for Stoke's SSX 3000 [128] configured as an LTE SeGW within an LTE/EPC test environment of two eNBs and EPC network elements built and supplied by ZTE, see Figure 47.

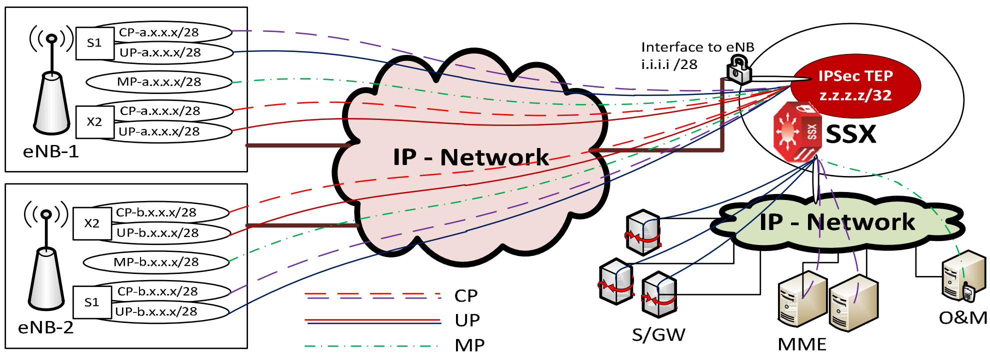


Figure 47 - LTE/EPC test environment.

The general aim of the testing was to study (on behalf of BT Wholesale):

- Impact of introducing an LTE SeGW into a public LTE/EPC network.
- Testing was conducted to fully understand possible deployment scenarios.
- Interoperability.
- Performance considerations.
- Finally, completely understand the possibilities of SeGW deployment within the LTE/EPC network.

To achieve this Stoke's SSX 3000 was configured to provide routing, IPSec Tunnelling and aggregation from the LTE network toward the EPC core. Testing was performed at BT laboratories in Adastral Park with the aim to demonstrate the SSX seamless connectivity to the supported services while also testing SeGW functions and other LTE/EPC network operations.

The following equipment, see Table 9, was used for test purpose in demonstrating commercial deployment scenarios of the SSX 3000 in BT's network providing IPSec Aggregation from the IP-RAN toward EPC network elements.

Table 9 - Test equipment list.

Core network:	**ZTE EPC (MME,S/P-GW)**	MME: ZXUN-uMAC V4.10.10 P3.B8 XGW: ZXUN-XGW V4.11.20 I9b HSS: USPP V4.11.10.P3.B3 PCRF: ZXUN-RCP V4.10.21.P1.B9
LTE network:	**ZTE eNodeB (2xeNB)**	H/W: BBU: 8200, RRU: R8880 S/W Phase 1: V2.00.050fP03_BT.0806 S/W Phase 2:
Security Gateway:	**1xSSX including (1x GLC + 1xIMC)**	H/W: SSX3000 S/W Phase 1: Stoke OS 4.6 S/W Phase 2: Stoke OS 4.6B1S2 (2010062215)
IPTN Transport Equipment:	**Routers:**	HW: ZXCTN 9000 V2.08.32R2 SW: ZXCTN 9000 V2.08.32R2B27
	Switch:	HW: ZXR10G-Series&8900&6900V2.8.02.C.43 SW: ZXR10G-Series&8900&6900V2.8.02.C.43.P12
Network Sync.:	GPS, IEEE1588, SyncE	
3 or 4x PCs:	laptops used as client, server, management, and troubleshooting tools	

Five test cases (deployment scenarios) were developed, described below in Table 10. These test cases first addressed basic functionality of the network as well as SSX security gateway features. Each test case was designed to demonstrate a scenario simulating commercial network deployments, which can be used by BT R&T to identify, recommend and demonstrate appropriate use cases for BT business units.

Table 10 - Test case description 0 to 4.

Test Case ID	**0**
Description:	Without the SSX in the data path.
Objective:	To use as reference for further tests.
Configuration:	ZTE EPC network without the SSX.
Test steps:	Open IP Packets are exchanged between eNB to EPC.
Test Success Criteria:	IP connectivity is achieved end2end.
Test Case ID	**1**
Description:	Single port at EPC edge and single port at Transport NW (Network). SSX communicates in open IP packets towards eNBs and to EPC, traffic flows transparently without SSX encrypting or modifying any packet. This modes SSX is used as a router.
Objective:	Verify that SSX does not incur additional delays, Packet loss, extra jitter, or reduction of bandwidth when traffic flows via itself; and is traffic that doesn't need to be modified/secured (e.g. synchronization packets). In this configuration the IEEE1588 PTP (Precision Time Protocol) may be applied before the SSX towards eNB, however

	the Ethernet Synchronisation used for PTP time reference of eNB should be injected after the SSX towards the eNB domain.
Configuration:	Refer to Proposed Network Integration.
Test steps:	Open IP Packets are exchanged between eNB to EPC. Run Benchmark test and compare results with reference (without SSX inserted in the test bed).
Test Success Criteria:	IP connectivity is achieved end2end.
Benchmark success:	Benchmark results and test scenario 1 results are considered similar enough to prove that SSX introduction will not have any negative effect on throughput, packet loss, delay, jitter, connection time.
Test Case ID	**2**
Description:	Single port at EPC edge and single port at Transport NW. SSX communicates using IPSec to eNBs and IP to EPC. Network is secured from edge of EPC to eNB completely.
Objective:	To demonstrate benefits / restrictions of introducing SeGW at Edge of network: • Removing / reducing the associated high processing task of terminating several IPSec tunnels from the S/GW (to overcome reported issues of S/GWs reduced performance due to the IPSec processing effort). The need for a secure tunnel between eNB and EPC (note there is a dependency on the mobile operator's method of deploying its backhaul network: • If the backhaul network is leased from a 3rd party, security is required to prevent the 3rd party having access to signalling and user data. • If backhaul network is owned by operator, but still it isn't considered secure enough, or equipment is located in untrusted premises. Security is therefore required to prevent the possibility of malicious intrusion (internal or external to the operator and trusted providers), breaking into the network and eavesdrop signalling and data traffic. • Using the SSX as an eNB aggregator, reducing signalling and providing EPC with 1 single point of attachment. **Drawbacks:** • The network becomes more rigid as nothing can be done to the traffic until it reaches the SSX in the edge of the EPC. No offloading, no edge caching, etc.
Configuration:	Refer to Proposed Network Integration.
Test steps:	Packets run from eNB to EPC. Run Benchmark test and compare results with benchmark (without SSX in the Test bed). Performance test.
Test Success Criteria:	IP connectivity is achieved E2E. IPSec tunnel is set up. IKE protocol to exchange a number of SA (Security Association) as the life time expires.
Benchmark success:	Benchmark results and test scenario 2 results are considered similar enough to consider that SSX introduction won't have any significant effect on: throughput, PL (Packet Loss), delay, jitter, connection time.
Test Case ID	**3**
Description:	Located in the middle of the transport network between two routers with redundancy (more than 1 connection/path to each router). SSX communicates using IPSec to eNBs and IP to EPC. Network is secured from SSX location to eNB only.

Objective:	To demonstrate benefits / restrictions of introducing SeGW in the centre of the transport network: • Removing / reducing the associated high processing task of terminating several IPSec tunnels from the S/GW (to overcome reported issues of S/GWs collapsing from the IPSec processing effort). • Distributing the SSX so more flexibility can be achieved (the location of the SSX becomes the first point where traffic can be offloaded; for example for edge caching, etc…). The need for a secure tunnel between eNB and the SSX in the middle of the transport network could be due to: • Edge of the backhaul network is considered more vulnerable to attacks and eavesdropping. • SSXs can act as an aggregator, reducing signalling and providing EPC with fewer points of attachment. • Due to dimensioning of the network e.g. 20k eNB in one country there may be a need to cluster eNB connectivity towards a security gateway aggregator such as the SSX before bringing back all the secure tunnels towards a number of core network centres. **Drawbacks:** • Leaves the connection between the SSX to the EPC vulnerable to intrusion. • More complex network design and management is required.
Configuration:	Refer to Proposed Network Integration.
Test steps:	Packets run from eNB to EPC. Run Benchmark test and compare results with previous benchmark results in other test cases and without SSX in the Test bed. Redundancy test (break default link and check connectivity is undisturbed, check PL).
Test Success Criteria:	IP connectivity is achieved E2E. IPSec tunnel is set up. IKE protocol to exchange a number of SA as the life time expires. IPSec tunnels seamlessly survive link failure.
Benchmark success:	Benchmark results and test scenario 2 results are considered similar enough to consider that SSX introduction won't have any significant effect on: throughput, PL, delay, jitter, connection time.
Test Case ID	**4**
Description:	SSX to act as two virtual security gateways connecting RAN Security Domain to Core Network Security Domain. Virtual SSX1 in the middle of transport network and virtual SSX2 at the edge of the EPC. Traffic is secured from eNB to edge of EPC.
Objective:	To demonstrate benefits / restrictions of introducing SeGW as two virtual gateways: • Remove / reduce the associated high processing task of terminating several IPSec tunnels from the S/GW (to overcome the reported issues of S/GWs collapsing from the IPSec processing effort). • Testing Virtualization capabilities of SSX, different SSXs inside 1 single physical SSX, useful when SSXs shared between different mobile operators. • Distributing the SSX so more flexibility can be achieved (the location of the virtual SSX1 becomes the first point where traffic can be offloaded; edge caching can be used, etc…). This option offers full security end to end and flexibility to act upon traffic before reaching EPC.

	Drawbacks: • More complex network design and management is required.
Configuration:	Refer to Proposed Network Integration.
Test steps:	Packets run from eNB to EPC. Run Benchmark test and compare results with previous benchmark results in other test cases and without SSX in the Test bed.
Test Success Criteria:	IP connectivity is achievedE2E. IPSec tunnel is set up. IKE protocol to exchange a number of SA as the life time expires.
Benchmark success :	Benchmark results and test scenario 2 results are considered similar enough to consider that SSX introduction won't have any significant effect on: throughput, PL, delay, jitter, connection time.

These tests (Table 10) provided the following results, Table 11:

Table 11 - Results for test case 0 to 4.

	Throughput (Mbps)	Delay (ms)	Jitter (ms)	MOS (Mean Opinion Score)	% Loss bytes
Scenario 0	22.52	19.45	13.75	4.33	0.019
Scenario 1	21.85	23.85	10.42	4.33	0
Scenario 2	23.8	25.67	10.42	4.31	0
Scenario 3	31.1	28.4	9.89	3.7	0.0465
Scenario 4	31.2	28.25	12.82	4.31	0.0133

The key performance indicators in these tests were delay, jitter and throughput, specifically the negative effects of the different network architectures on them when compared to Scenario 0.

Because the tests showed little or no impact in throughput and jitter, the attention was focussed on delay. The effect of adding a SeGW introduces a 4.4ms delay between scenario 0 and 1, while enabling IPSec tunnels into the network introduces a 6.2ms delay between Scenario 0 and Scenario 2 and only 1.8ms delay between scenario 1 and 2, these increases of delay are due to the processing cost of IPSec in this specific equipment. Scenario 3 was used to demonstrate the support redundancy on link failure between eNodeB and SeGW by providing a secondary redundant network path and the effect of this seems to add 2.7ms delay. Scenario 4 was used to prove that the SeGW can be virtually split enabling support for multiple MNO's on a single physical SeGW without any negative effect on delay or throughput.

- **Scenario 0:** Network end-to-end validity was proven without the SSX SeGW by studying Service (Ping) latency.
- **Scenario 1:** SeGW can be configured to let traffic through in transparent mode i.e. traffic passes through unencrypted and no packet modification occurs.

- **Scenario 2:** IPSec tunnels turned on between SeGW and eNBs. Comparing the throughput for scenario 1 and 2 proved evidence for service continuity and end to end throughput performance. A level of IPSec overhead (see Figure 48) was observed looking at the throughput results either side of the SeGW. Phase 2 testing will consider IPSec overhead in further detail considering the effect of IPSec on different protocols.

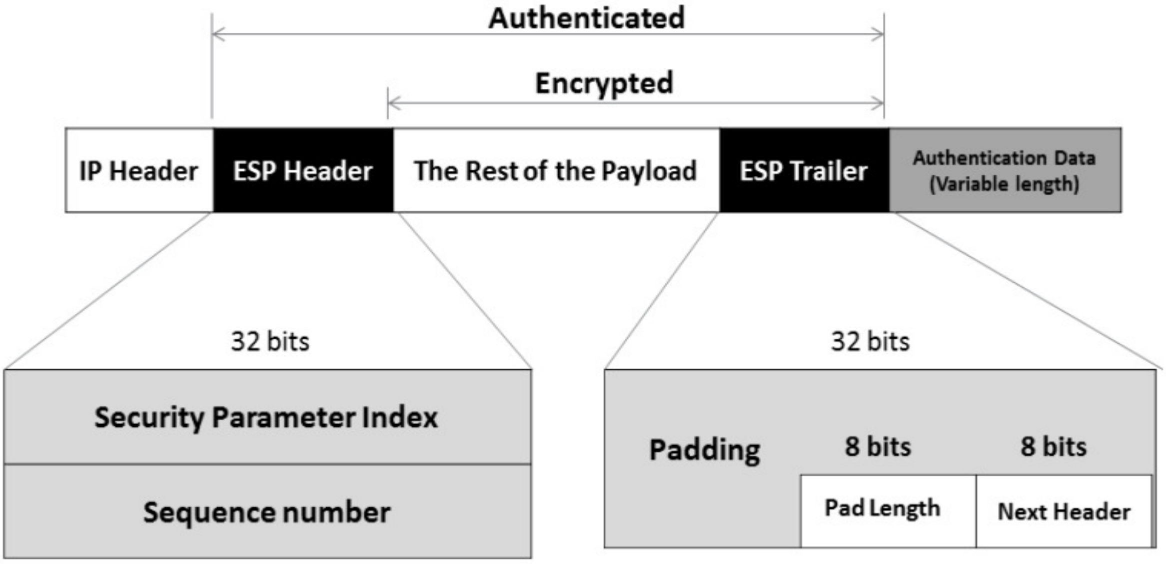


Figure 48 - IPSec encapsulation in ESP mode (Source: [126]).

- **Scenario 3:** Confirmed path redundancy can be added in case of link failure between eNodeB and SeGW. Redundancy tests where successfully demonstrated providing service continuity for VoIP, Internet connectivity and data streaming with IPSec tunnels configured between the eNodeB and SeGW using S1 interface.
- **Scenario 4:** Testing proved a virtual split of the SeGW in 2 between the edge and core of the network. This created virtual routers within the same equipment by creating IPsec and normal IP routing and connections in different parts of the network, whilst maintaining the same level of service.

5.4.4. Phase 2 Testing Scenarios

The phase 2 test scenarios use the same test environment as illustrated in Figure 47, although these tests are investigating in more detail key functions in the network: SeGW, eNodeB and Handover.

Firstly, the performance of the SeGW is examined, in particular the percentage overhead of using an IPSec tunnel on different application protocols and looking at varying packet size. Followed by investigating the performance of the eNodeB to see how many IPSec tunnels it can support and how the increase of tunnels effects CPU (Central Processing Unit) utilisation and throughput. Lastly, exploring and evaluated the different types of handover e.g. X2 direct (eNodeB to eNodeB), X2 via SeGW and S1 handover.

The general aim of these tests is to provide:

- Justification of the need and advantages of distributed Security Gateways to underpin the BT Wholesale intelligent backhaul opportunity.
- An understanding of the LTE SeGW and if the IPSec tunnel overhead is likely to cause impacts within the network.
- Insight into the performance of the eNodeB, in particular how the increased number of IPSec tunnels may affect it.
- Comparing speed and efficiency of Handover in order to determine if X2 direct handover is a viable option for the distributed SeGW solution and if it could provide potential bandwidth savings to the SGW and reduced handover latency compared to that of a standard S1 handover.

The results of these tests provided the following conclusions:

- **Scenario 1:** Considered SeGW performance and IPSec Overhead considering different types of traffic e.g. VoIP, HTTP (Hypertext Transfer Protocol), UDP, RTSP (Real Time Streaming Protocol) and looking at varying packet sizes, see Figure 49 and Figure 50.

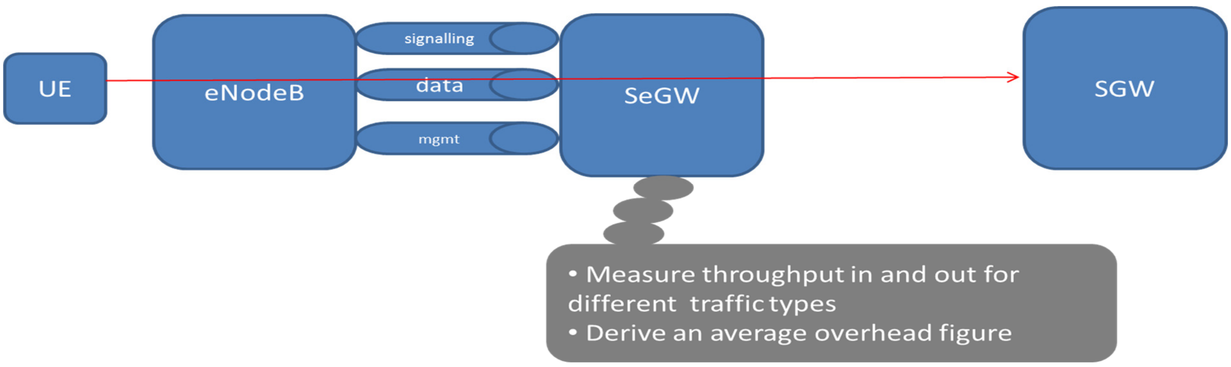


Figure 49 - Scenario 1 - IPSec tunnel overhead.

The investigation proved that the IPSec overhead for different types of traffic behaved in a similar manner, except where payload sizes for particular protocols (e.g. RTSP, VoIP) showed large variation resulting in large packet size variation, see Table 12. However, the main contributing factor to the increase of IPSec overhead was the decrease in packet size, as seen in Figure 48, IPSec adds at least 64 bits no matter what the size of the original packet is an therefore smaller packets have a bigger impact, see Table 12. Results for UDP traffic are shown below against different payload sizes. As packet size range increases also does the SeGW efficiency.

Table 12 - Jperf results on different UDP packet size.

UDP Payload Packet Sizes	eNodeB to SSX (ESP) Average Packet size	SSX to EPC (GTP) Average Packet size	Overhead due to Packet Size	Average Bytes/Sec eNodeB to SSX (ESP) (Wireshark	Average Bytes/Sec SSX to EPC (GTP) (Wireshark Summary)	Percentage overhead from IPSec	SSX % efficency	Tester
1330	1471	1405	4.5	1390004	1323828	4.8	95.2	jperf
1024	1170	1101	5.9	1434794	1345432	6.2	93.8	jperf
512	661	590	10.8	1619813	1442869	10.9	89.1	jperf
256	406	334	17.7	1991333	1637914	17.7	82.3	jperf
128	278	206	25.9	2726133	2019850	25.9	74.1	jperf

Packet headers SSX to EPC
Payload + 8 byte UDP header + 20 byte IP + 16 byte GTP + 20 bytes IP + 14 bytes Ethernet header= 78 bytes total header.
Packet headers eNodeB to EPC
payload+ 20 bytes IP header + 18 Ethernet header & trailer + 50 ESP = 88 bytes overhead for IPSec + padding

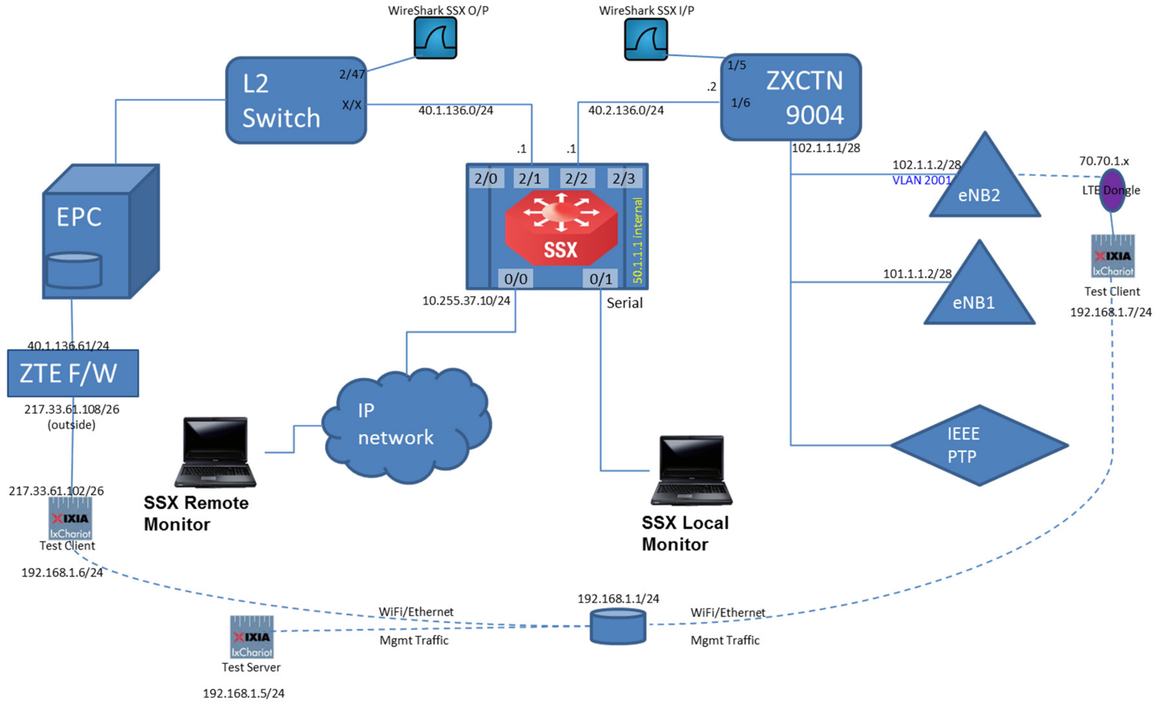


Figure 50 - Scenario 1 network diagram (Ixia).

- <u>**Scenario 2:**</u> investigating eNodeB performance by concluding how many IPSec tunnels may be supported and the likely degradation for multiple IPSec tunnels and their effect on CPU utilisation and throughput, see Figure 51 and Figure 52.

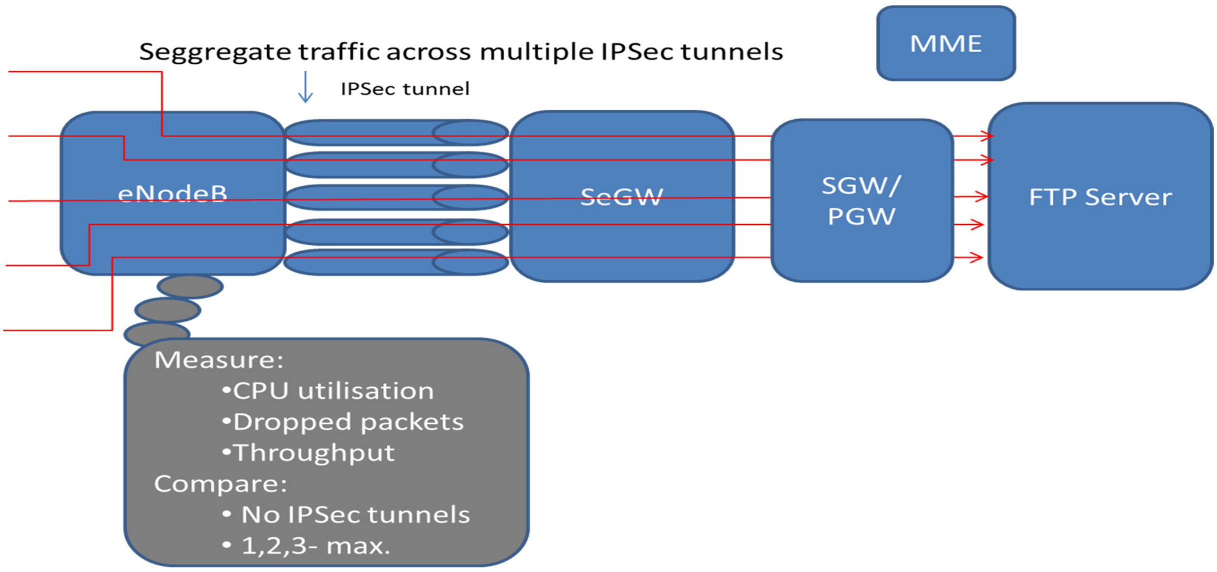


Figure 51 - Measuring eNodeB performance with varying numbers of IPSec tunnel.

Our eNB implementation was proven to support up to 10 IPSec tunnels with minimal impact to CPU and performance, see Figure 53. No more than 10 IPSec tunnels can be supported (which may be required in small cell environments). Also, when eNodeB processing boards are fully utilised we would expect to see some impact on performance due to the IPSec processing required.

- Tests showed there is no impact or correlation between throughput and the number of IPSec tunnels.
- There is only a slight increase in CPU for the Control board (CC board) as the number of IPSec tunnels increases, due to underutilisation of the Process Board as only supporting 1 CC board/sector and not more. In a live network with full utilisation we would expect to see a higher CPU difference with the tunnels. The Control Board (CC board) controls the IPSec encryption/decryption process and so it is these figures we need to consider when comparing CPU and the number of IPSec tunnels.

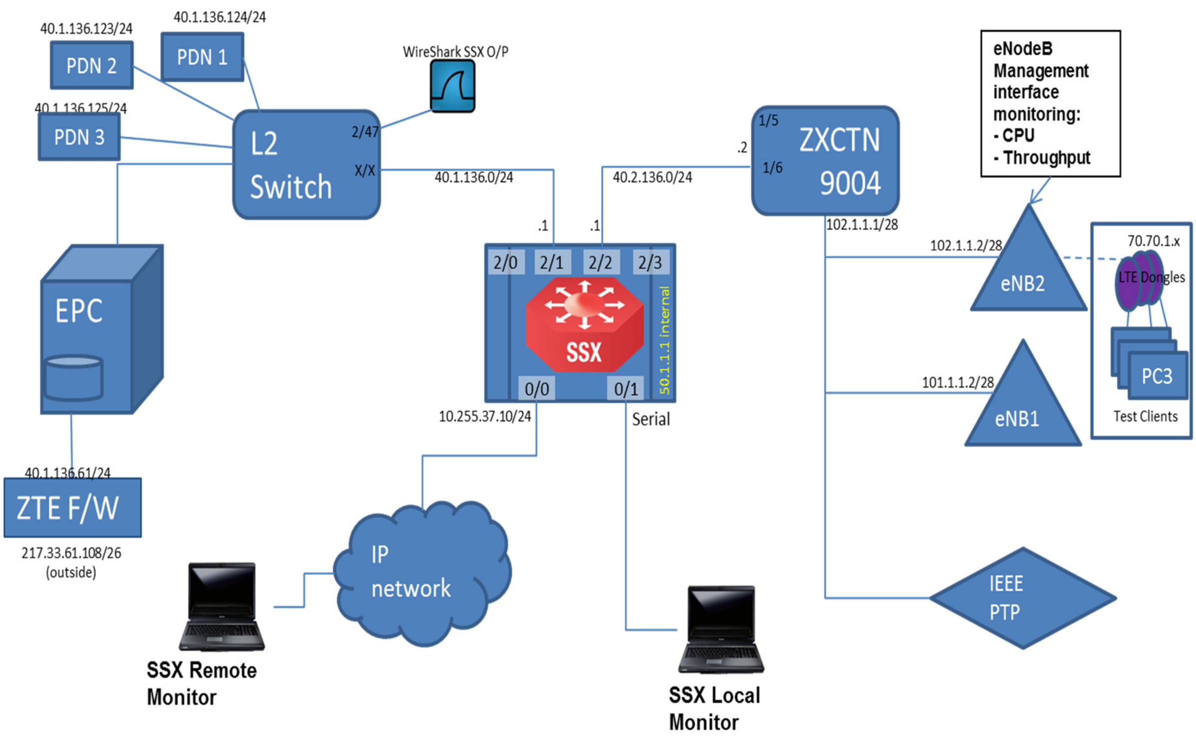


Figure 52 - Network layout for scenario 2 tests.

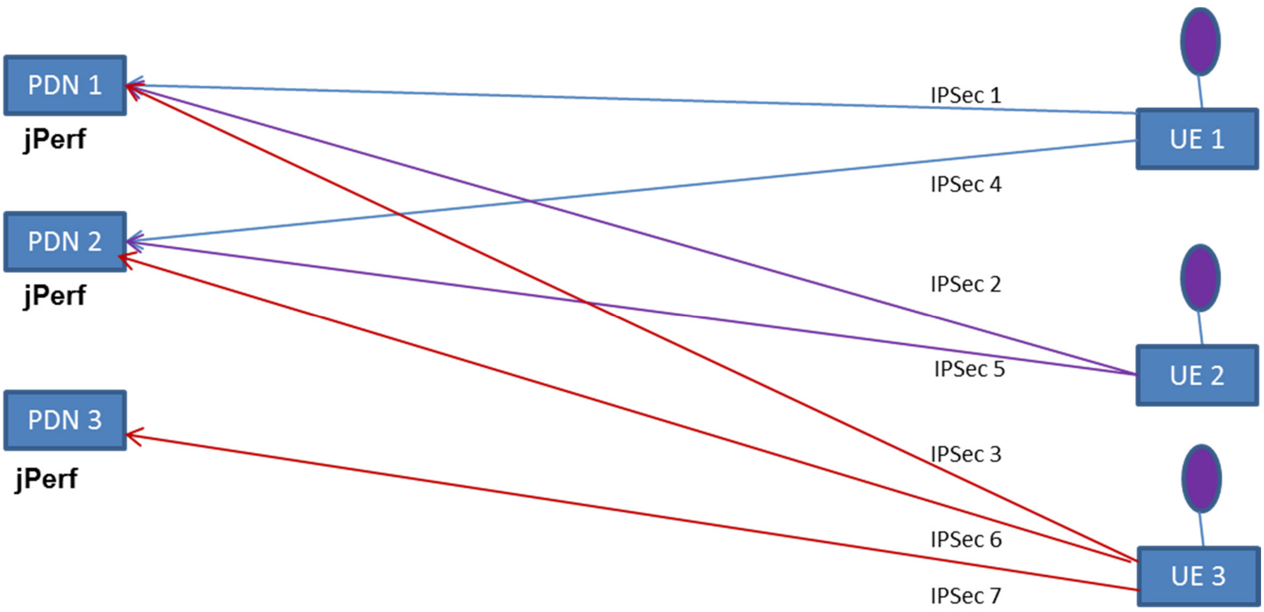


Figure 53 - PDN server to UE mapping showing data (User plane) tunnels used in scenario 2.

Table 13 - CPU utilisation and throughput results compared for a different number of IPSec tunnels.

Total Bandwidth sent Mbps	UDP Packet Sizes (payload)	Number of IPSec Tunnels	Traffic split	Average Throughput through Tunnel(s)	CPU Processor Board	CPU CC (Controller Board)	% Av. Pkt Drops at client(s)
100	1024	0	50 Mbps x 2UE's	96.2	26.20%	16.10%	0.0%
		1	50 Mbps x 2UE's	101.5	23.20%	16.10%	0.60%
		3	35 Mbps x 3UE's	94.1	23.80%	16.30%	5.00%
		7	14 Mbps x 7 tunnels **	93.9	26.60%	16.70%	4.70%

** 7 tunnels 100 Mbps (7 x 14 Mbps) - UE1 14 Mbps x 2, UE2 14 Mbps x 2, UE3 14 Mbps x 3

CPU process board's CPU is only affected by throughput so these results do not need to be considered, see Table 13.

On the other hand the number of tunnels has an impact on the throughput as not only the IPSec headers need to be considered but also the tunnel headers. This can be observed in Figure 54 below.

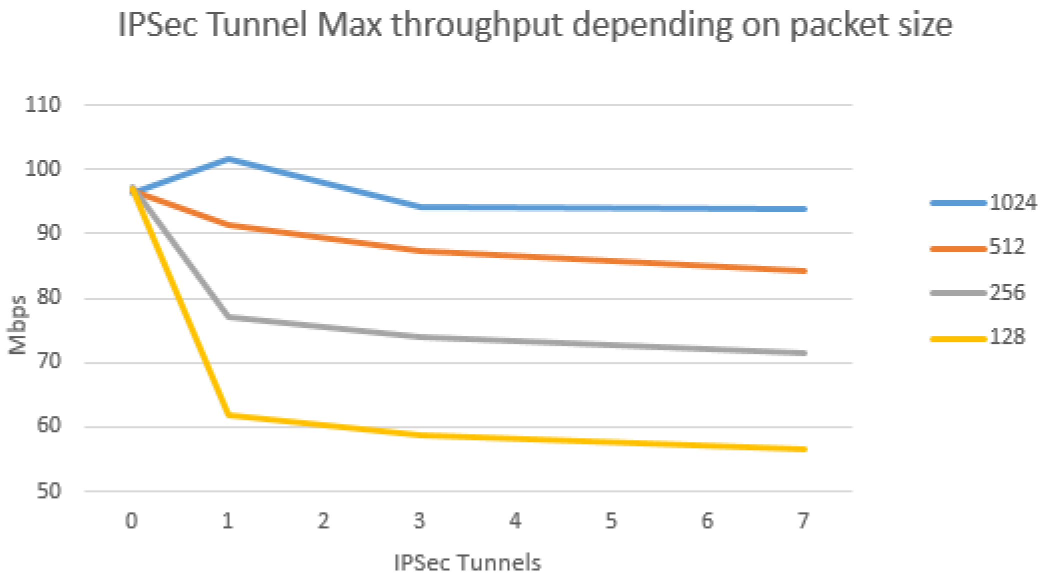


Figure 54 - IPSec maximum throughput depending on packet size.

Notes: One Process Board can Support 3 sectors (3 Controller boards) so we are underutilised during these tests as only have one sector configured. So the process board is never overloaded because of too many sectors.

- **Scenario 3:** Comparing speed and efficiency of the different types of handover: S1, X2 (both via the SeGW) and X2 direct, see Figure 55 and Figure 56.

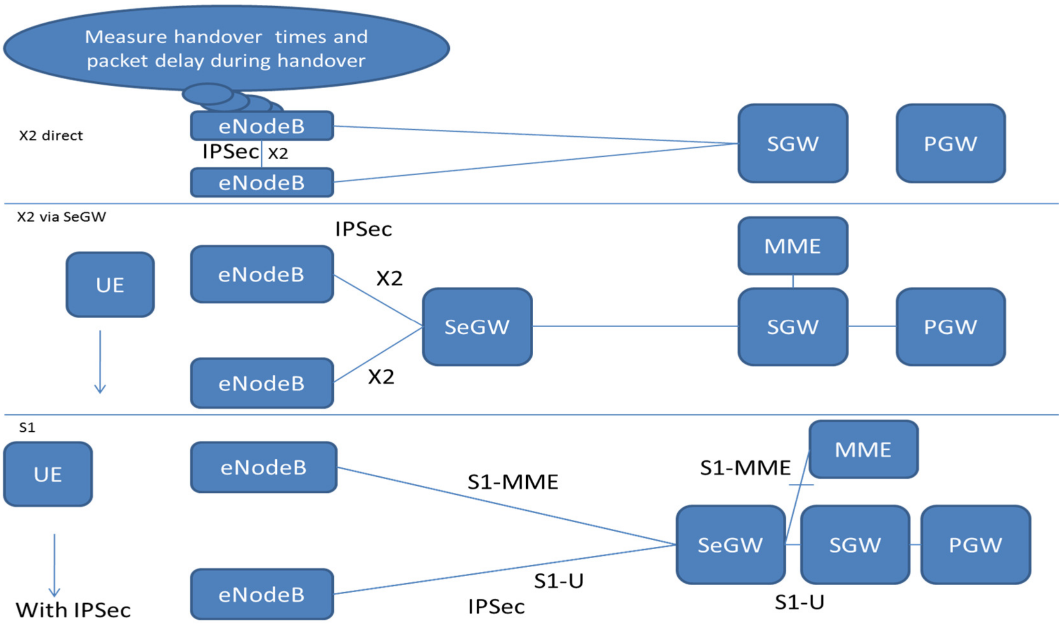


Figure 55 - Scenario 3 – Handover.

- It was proven that X2 direct showed a faster handover followed by X2 via the SeGW and S1 via the SeGW. Although, the handover times for the S1 and X2 interfaces via the gateway were fairly close, in a live network environment the time savings for X2 either via the SSX or direct would be more apparent than the S1 handover.
- Different use cases (via S1, X2 via SeGW, and X2 direct) have been compared for handover performance by different interfaces X2 and S1 [129], proving that X2 based handover works. In a real network deployment we would expect a difference between X2 and S1 based handover with a minimum of 8-10ms based on the Cornwall LTE trial (on an uncontended backhaul, more on Section 5.1).

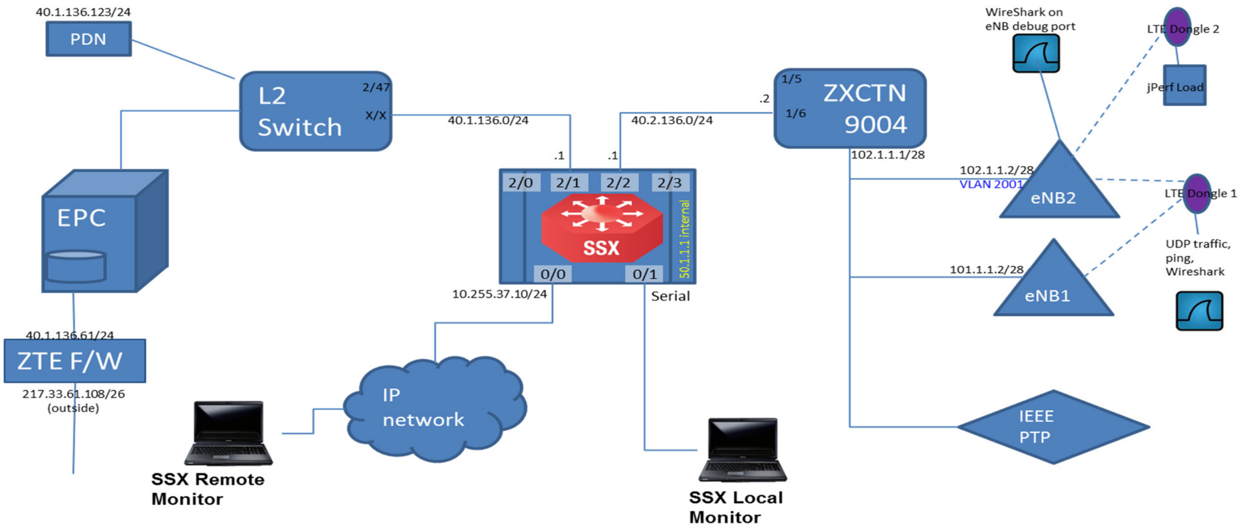


Figure 56 - Detailed network diagram for handover tests.

5.4.5. Summary

The study has proven both the flexibility of SeGWs in terms of placement within a mobile network and their key benefits:

- As a tunnel aggregation point, improving scalability and performance of Core EPC components (SGW/MME), which typically are affected when IPSec tunnelling is enabled.

- The introduction of a SeGW and IPSec tunnels into the network is 6.2ms delay. It has also been demonstrated that the eNodeB and SeGW support redundancy on link failure. In addition the investigation has proven that the SeGW can be virtually split enabling support for multiple MNO's on a single physical SeGW.

- By placing them close to the edge of the network potential for value-adding services such as traffic offload, content ingestion and content re-insertion. As well as helping with mobile monitoring and optimisation tools.

- IPSec processing overhead reduction on eNodeBs for X2-based handovers, which reduces handover latency so relieving processing demand on the core. Also, as shown in our study an X2 based handover via the SeGW has lower latency than that of a direct X2 handover where IPSec is established between the neighbouring eNodeBs.

- Different use cases have been compared for handover performance by different interfaces X2 and S1, proving that X2 based handover works. In a real network deployment we would expect a difference between X2 and S1 based handover with a minimum of 8-10ms based on the Cornwall LTE trial (on an uncontended backhaul).

- Our eNB implementation was proven to support up to 10 IPSec tunnels with minimal impact to CPU and performance. No more than 10 IPSec tunnels can be supported (which may be required in small cell environments). Also, when eNodeB processing boards are fully utilised we would expect to see some impact on performance due to the IPSec processing required.

By looking to harness some of the flexibility and efficiency demonstrated by SeGW in this study, obvious key business opportunities are available to both BT for MEAS (Managed Ethernet Access Service), WCC (Wholesale Content Connect) and value-adding services as well as key benefits to MNO's outsourcing their SeGW. Benefits to BT include:

- Offer additional value, exploit up-sell opportunities if sold in conjunction with MEAS.
- Enable WCC for mobile (e.g. place CDN (Content Delivery Networks) and point of content injection closer to the edge).

- Enable future opportunities to deliver value-add services (e.g. Service LAN).

BT is natural option for MNOs who decide to outsource their security GWs, which could be located at MEAS aggregation points. Cost savings and scalability improvements to the MNO could be provided by:

- Sharing Security GWs – Phase 1 scenario 4 proves virtualisation of Security GWs as well as traffic segregation.
- BT may be able to offer optimal locations for Optimisation of Network topology:
    - Traffic offload.
    - X2 IPSec tunnel termination.
- If BT provided a shared EPC to MNOs – SeGWs would be very likely be hosted as part of the overall solution.

Chapter 6: Content Distribution

In order to deliver better latencies in a 5G world we need to shorten the distances between the content and the subscriber, this can be achieved by moving the core functionality of the wireless network closer to the radio access network and virtualization and core distribution will play a big hand in allowing that, but at the same time content distribution needs to be allowed to get closer to the subscriber.

These following tasks concentrate in this last idea, and deliver improvements to the current methods used for content delivery in mobile networks.

6.1.State of the Art (2011)

CDNs are used to improve network performance by [130]:

- Improving accessibility, by bringing the content closer to where it is requested.
- Maximize bandwidth, by delivering the content within the bandwidth constraints experienced by the subscriber
- Delivering a right copy of the content they replicate from the original sources.

The typical functionalities of a CDN are:

- To manage networks components and provide reporting, monitoring and accounting of content delivery in the network.
- To negotiate the content requirements of a subscriber or group of subscribers.
- To replicate or cache content from the original sources so it can be more efficiently distributed.
- To redirect and deliver content to subscribers from the closest most suitable CDN cache server.

There are two general ways to organize a CDN [131], the overlay approach and the network approach. In the overlay approach, the CDN servers are placed on the back of the core networks and the core network doesn't play an active role in the content delivery. In the network approach, the core routers and switches are equipped with code and policies to handle the content and optimize its delivery.

The closer the content delivery servers are to a customer, the faster and more reliable this content can be provided [132]. In Section 6.2, we explore the delivery using Saguna edge cache servers which can be located in between the RAN and the Core network to provide a much shorter delay and improve backhaul and radio utilization. In Section 6.3, we propose a new architecture which not only takes into account the location of the content but also the location of the user and can change the user data path within the mobile network to optimize the content delivery.

6.2.Saguna Testing

It was decided to test a solution from a 3rd party company called Saguna which provided improved content delivery to understand the current content optimization techniques used and the latest developments [133].

The main techniques in use are;

- Transcoding: Change the codification of the content (or serve same content with different codification) based on network conditions, QoS, device and screen capabilities.
    - Adaptive Bitrate Streaming: This technique may utilise protocols information such as TCP and RTCP (Real-Time Control Protocol) in order to deliver on the fly re-encoded content. The re-encoding process takes into account existing variable network conditions - user's bandwidth and CPU capacity in real time and adjusting the quality of a video stream accordingly. Effectively this uses transcoding. It requires the use of an encoder which can encode a single source video at multiple bitrates.
- Transrating: Strictly speaking transrating involves modifying the encoding rate for some content. This operation involves re-coding (using the same codec).
- Bitrate Throttling: The content is served at “consumption speed” so that bandwidth is not wasted, may involve buffer management, TCP Optimisation, bandwidth shaping, and/or video encoding rate.
- Modification: The content may be optimized, e.g. dropping video frames may enhance user experience on some devices.
- Traffic Prioritization: Traffic may be prioritised so that the most important content is delivered in an efficient manner. A combination of DPI (Deep Packet Inspection) and policing is usually required.
- Cache: Serving content from a closer to the edge/user repository.

The technique used by Saguna uses several of the above mentioned techniques, but the main one is the cache. Cache can provide savings on bandwidth support at backhaul, core and internet peering, since the cached traffic will not need end-to-end delivery from the content originator. Caching nodes are good points of entry to monitor the traffic, this allows to architect the network in order to address those traffic patterns.

Parameters or points that need to be taken into account:

Cache-Hit ratio: This is the percentage of content served from the cached memory.

Average size of objects served: A high cache-hit ratio cannot be translated automatically into a high percentage of traffic being served. This will depend in general on the size of the objects that are being served.

Position of the cache on the network: The closer to the user the content is found, the bigger amounts of savings that can potentially be generated at backhaul, core and peering. However, as the solution is deployed closer to the user the cost of deploying edge cache increases.

Cache System Architecture: Centralised versus Distributed. Edge cache typically needs to be distributed.

Transparent versus re-direct: In a re-direct cache/CDN system the client receives an order to re-direct its request for content to the original content holder towards a different local repository where the content is stored. Transparent cache does not require for the client to issue a new request.

6.2.1. Saguna Solution

Their solution is based on catching the content that goes through their nodes which are located within the network operator. These "caching nodes" have got intelligence to create copies of the most requested content from the subscribers they serve. After this copy is created instead of going to the original source site for the content, the content is served from the Saguna node to speed delivery, latency and lower network costs. Moreover a controller in the core network allows Saguna edge nodes to share content between themselves without the need to access the content from the original source. Saguna claim an up to 70% saving in backhaul costs alone [134]. In trials with live mobile operators, Saguna has proven an improvement of 50% on backhaul utilization and 20% in radio utilization [135].

With the help of Saguna, it was possible to integrate their solution into a BT Research LTE network, in the same architecture as described in Figure 57.

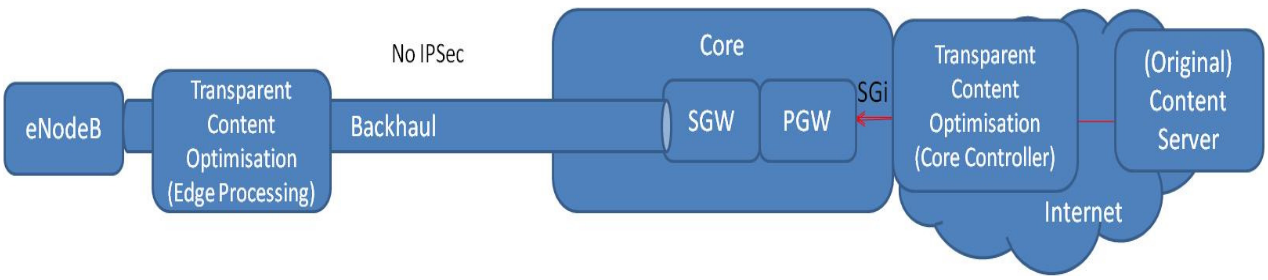


Figure 57 - Saguna basic architecture.

6.2.2. Test scenarios

For scenario 0, the LTE/EPC network without Cache Solution was desired to use it to compare performance results with the other scenarios. In this scenario the average delay to the PDN GW (Packet Data Network Gateway) was 34ms and the jitter was 21ms.

In scenario 1, see Figure 58, the Saguna Cache solution was inserted but working in transparent mode (without using the actual cache) which lets traffic through without modifying it. Tests on latency and jitter on the S1 interface gave very similar results to scenario 0 with a delay increase in the order of hundreds of microseconds.

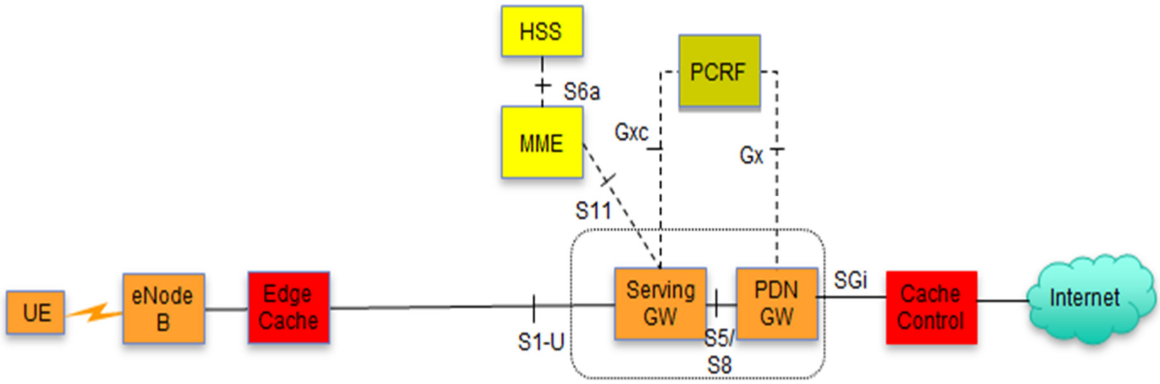


Figure 58 - Scenario 1, 2, 3 architecture.

Scenario 1: Edge Cache in transparent mode.

Scenario 2: Edge cache enabled.

Scenario 3: Bitrate Throttling in edge cache enabled.

Finally in scenario 2 the Saguna Cache solution is enabled. Here the tests on delay and jitter still seem not to affect (increase in the order of hundreds of microseconds). The delay and jitter were tested in peak conditions without any effect.

In scenario 3, a radio utilisation enhancement from Saguna through bitrate throttling which they claimed provided a 20% enhancement was tested. To enable it, in the PCRF a rule to limit the maximum bandwidth to 4Mbps was enforced, and with the clients connected to one single eNB, simultaneous YouTube videos with resolution of 640 x 360 24fps (about 500kbps) were started, this means that as a theoretical maximum a single user could only see 8 videos before starting to see errors/breaks in the videos. In the testbed, without bitrate throttling only 5 videos could be seen without errors/breaks, once the Saguna technique was enabled up to 7 simultaneous videos were possible. This gives an improvement of over 40% (Saguna claims it could go up to 70%), see Table 14, so if we assume (according to Saguna data) that up to 50% of the content at peak times can be served from the Cache, we expect to see a 20% more video sessions running smoothly by using Bitrate throttling which leads to quality of experience improvements. Also assuming that 50% of all mobile data traffic is video we can expect a 10% improvement in radio utilisation over all traffic.

Table 14 - Simultaneous videos without error/breaks.

	Simultaneous videos without errors/breaks	Improvement
Without Saguna	5	0%
With Saguna	7	40%

At the same time during those tests the traffic as measured in the backhaul had less spikes which makes it more predictable and easier to manage for the operator, see Figure 59.

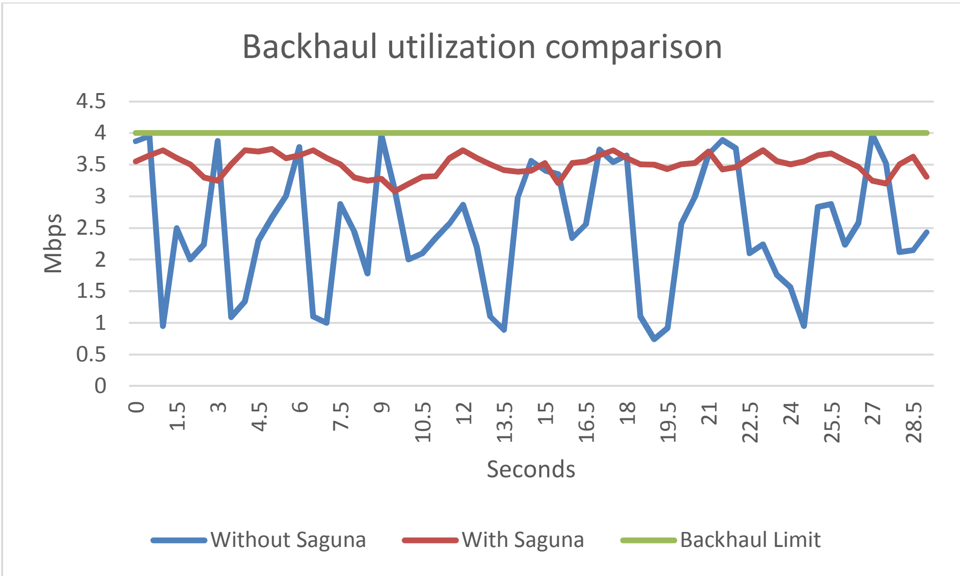


Figure 59 - Backhaul utilization comparison with and without Saguna.

Saguna edge cache has a better knowledge of the content that is being transmitted and therefore can send it at the most appropriate rate to allow for a better backhaul and radio utilization.

6.2.3. Summary

In an unsecured backhaul network, Saguna technology can deliver its promises. Because of the open standards used in LTE, backhaul data is less protected than in previous 3GPP technologies, see Section 5.1, therefore 3GPP mandates the encryption of all signalling and recommends the encryption of user data, see Section 5.4.

The issue with this type of solution is that it requires inserting the Edge cache node (see Figure 58) in between the eNB and the core network, as compared with traditional solutions that only appear after the SGi interface behind the PGW, see Figure 60. If IPSec is used(as described in Section 5.4), which will be required for traffic coming from small cells, then all content requests will be encrypted and traffic cannot be served from the Edge cache. To break this, what was proposed was to place a SeGW closer to the edge of the RAN to enable Content Cache savings, see Figure 60.

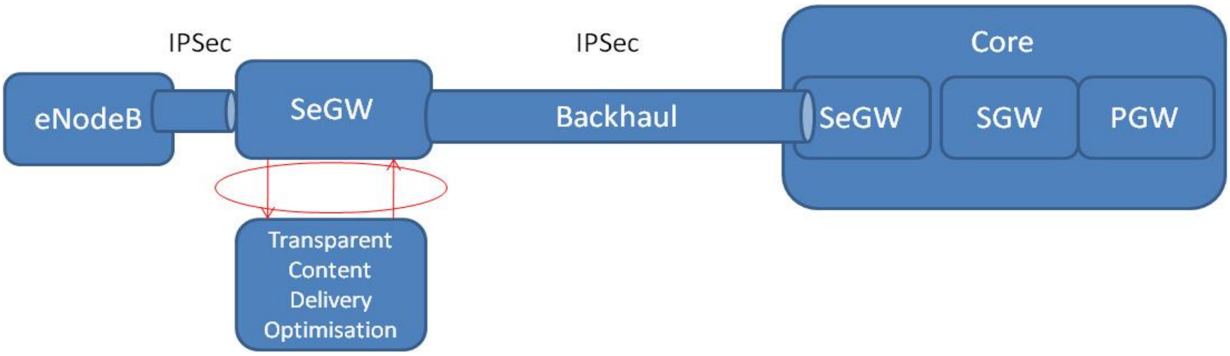


Figure 60 - Edge content cache collocated with edge SeGW.

Traffic can then be re-encrypted if necessary towards the core network, although this might not be necessary if the backhaul used is considered secure from the edge SeGW.

Also if a DPI node is inserted with a local PGW function it would be possible to achieve IP offload and optimized traffic routing, see Figure 61, which together with the edge cache can bring the latencies in mobile networks much closer to the expected 5G values.

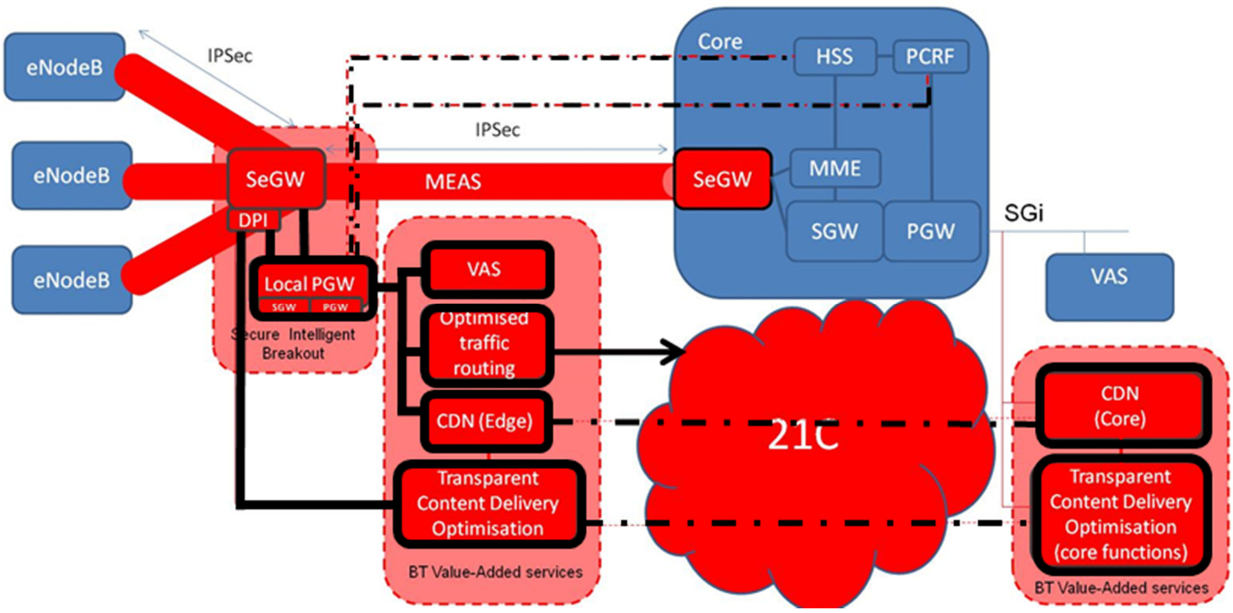


Figure 61 - Edge SeGW providing local breakout.

In the next section an idea to handover to the different multiple local PGWs depending in the content location to avoid long delivery paths and diminish delay.

6.3.Content-Aware GW Re-Selection – Patent Filed 03/2013

Within cellular data networks, the typical architecture includes an access network of cellular base stations connected to a network core via gateways. Data packets are then transported across the core to external networks such as CDN, see Figure 62.

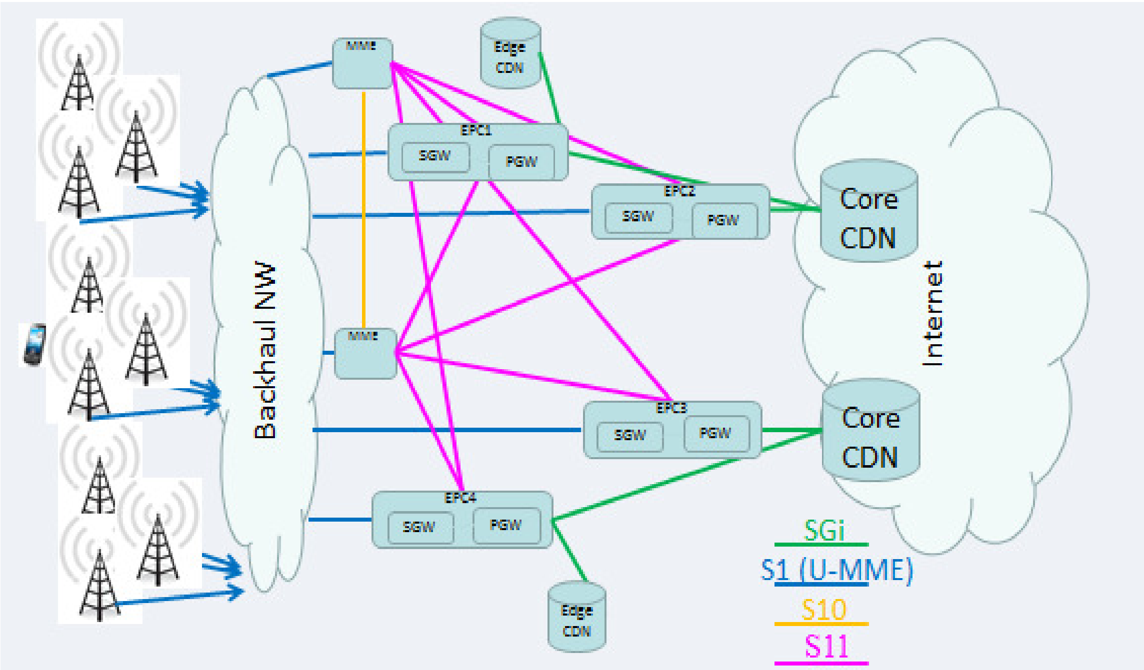


Figure 62 - Standard mobile network connectivity and cache solutions.

As usage of the networks increases, there is a need to optimise the flow path of data across the various parts of the network. Content cache techniques rely on data replication and locality to improve the accessibility to data. In this way, a requesting device can be redirected to the closest cache in the data network which contains that data.

Whilst caching can improve the speed of data retrieval, in such conventional networks, there is no further optimisation of the data path. So the following case could occur, see Figure 63:

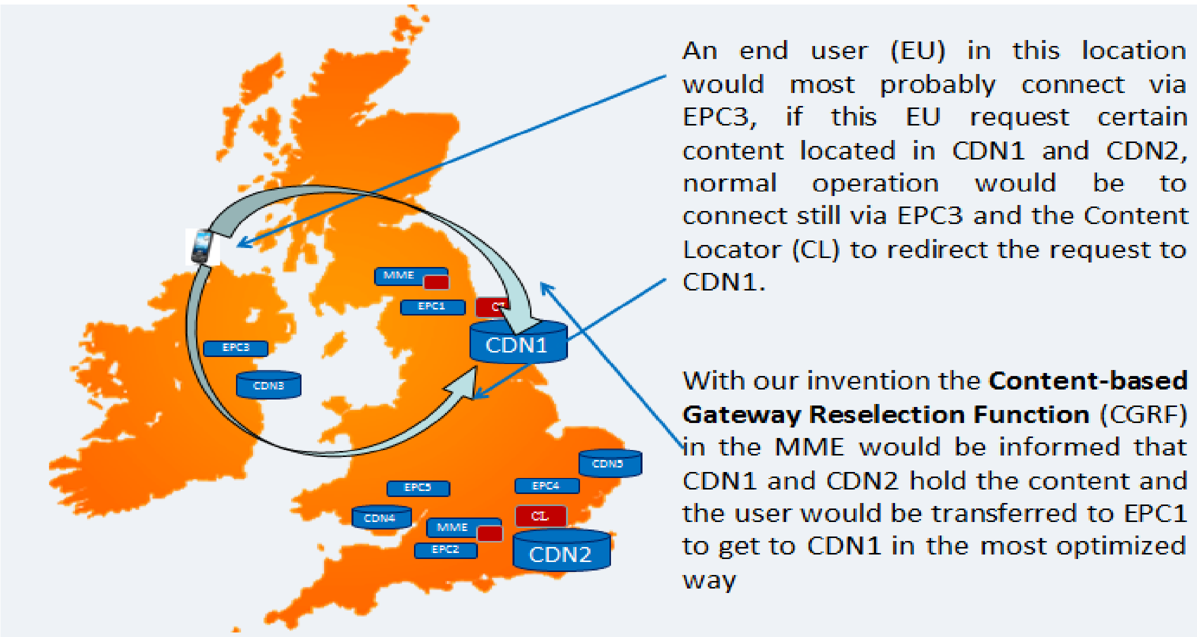


Figure 63 - Issue of content not available in current EPC CDN.

6.3.1. Patent Summary

In our invention [8], we introduce a CGRF (Content-based Gateway Reselection Function), this entity, located in the MME (see Figure 64), is responsible for moving the data connection between the user device and the gateway pair (SGW/PGW) initially selected and a new pair if it determines that the data connection would be more efficiently this way.

Another element needed is a NLS (Network Location Server) which stores details of the network location (i.e. IP address) and geographical location of each component (PGW, MME, CDNs, etc) in the network as well as the overall network topology. It is accessed by the CGRF to use this information to decide the best routing for each end user device.

Finally, a CL (Content Locator) which is responsible for maintaining a directory of where content is located; for intercepting user device requests for information and if the content is available within the content delivery network, redirecting the content request to an appropriate content delivery cache. The CL also provides information to the CGRF so that the CGRF can optimise the path between the user devices and content delivery caches via an appropriate gateway pair (SGW/PGW).

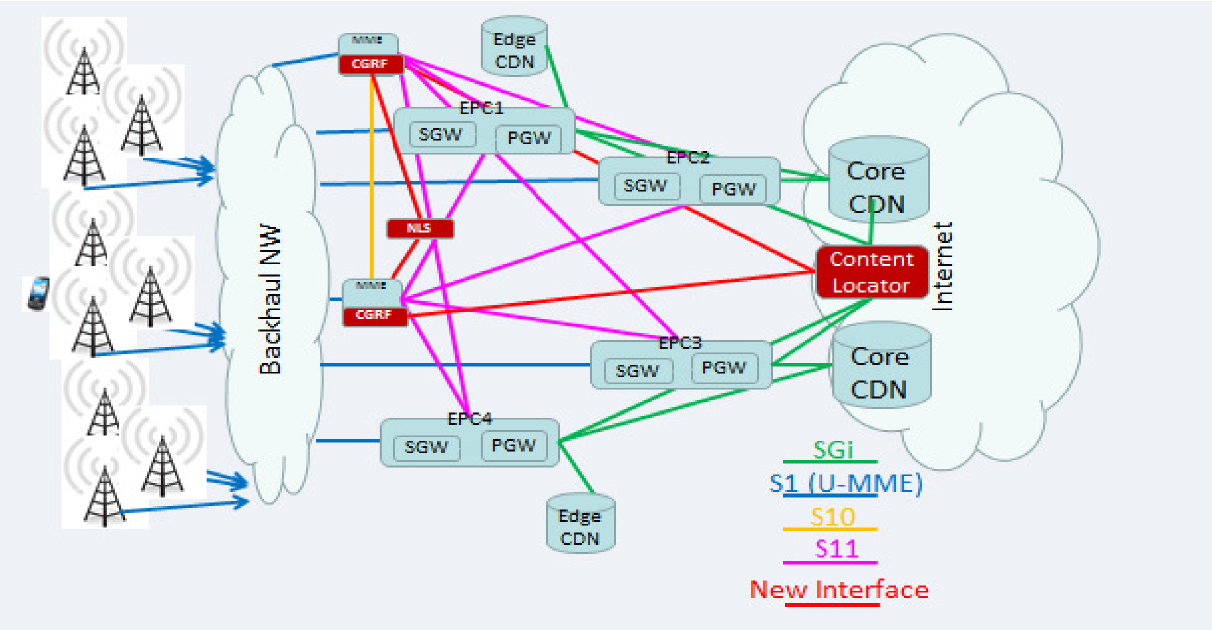


Figure 64 - Standard mobile network with new elements required for patent solution.

6.3.1.1. Example Use Case

The following steps describe a possible use in a mobile network. The steps below coincide with the ones relating to Figure 65 (next page):

1. User is connected and authenticated to the network

2. UE sends a request for a piece of content to a remote server located on the Internet

3. This message is intercepted by the CL enroute to the remote server. The content locator sits on the path between the PGW and the core network so it can read all traffic flowing through the PGW in a similar manner to deep packet inspectors.

4. CL checks the CDN and specifically the edge and core content delivery caches, to see whether the requested content is available and therefore could be delivered to the user device from one of the content delivery caches. In the example, core content delivery cache and edge content delivery cache have cached the requested content.

5. Instead of simply redirecting the user device's request to the nearest content delivery cache as is conventional, the CL helps the CGRF improve the overall routing of data connection between the mobile device and the content delivery cache. It then sends a list of the content delivery caches containing the requested content to the CGRF within the EPC.

6. The CGRF uses knowledge of the geographical locations of the gateway pairs, content delivery caches and the user device, as well as routing costs, to determine a nearest content delivery cache and the associated gateway pair within the EPC that would best serve the content request to the user device. In this example, the edge content delivery cache contains the requested content and has a lower routing cost towards the mobile device.

7. The MME moves the PDN session to the new gateway pair and the CGRF notifies the content locator that the edge content delivery cache was selected to serve the requested content. The MME can use procedures such as TS23.401 Selected IP Traffic Offload (SIPTO) [136].

8. The content is served from the new GW and cache

The processing of content locator and CGRF allows for data sessions between user devices and content delivery caches in a content distribution network via an EPC to move independently of the location of the content delivery caches containing the requested content. In this way, the path between these network components can be optimised thereby improving the operation of the network as a whole.

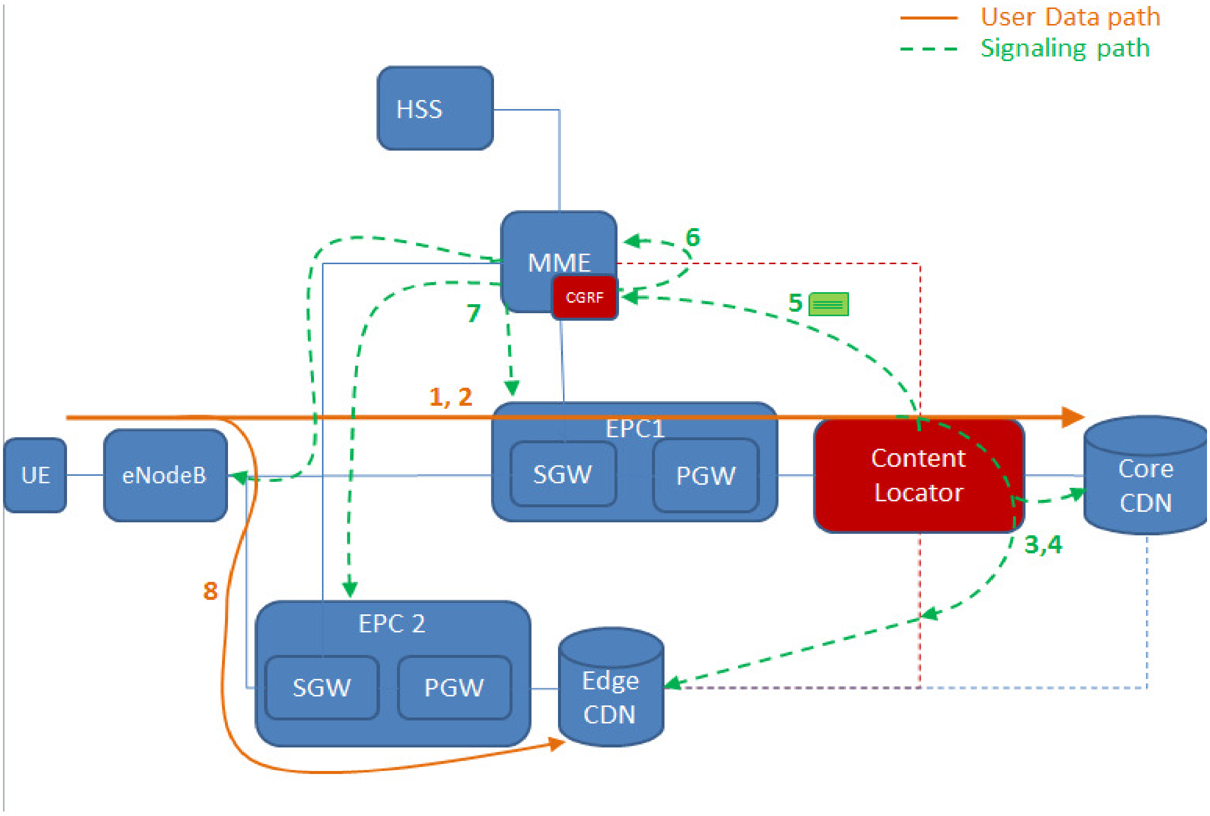


Figure 65 - Step by step flow on a mobile network.

6.3.2. Possible Implementation

The following algorithms and flow charts were presented as part of the patent application as an example implementation of the solution for the Content request flow and the CGRF and CL internal algorithms.

6.3.2.1. Content Request Flow

In Figure 66, we can see the process flow of a normal content request and how it interacts with the different described elements in the network.

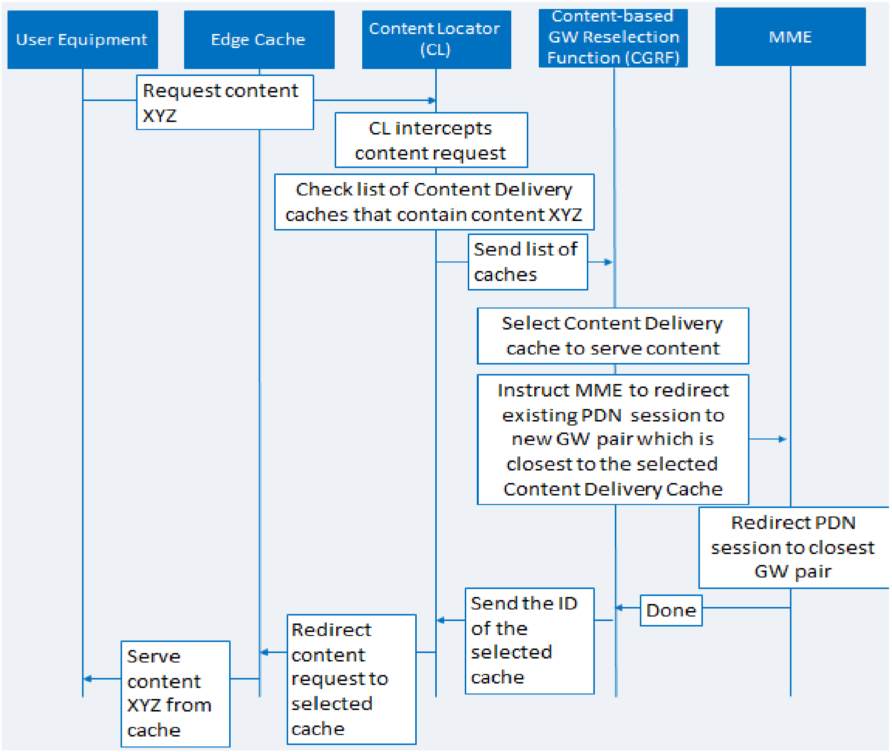


Figure 66 - Content request flow.

6.3.2.2. CGRF Algorithm & CL Algorithm

In this section we can see CGRF and CL algorithm examples that explain them step by step, Figure 67.

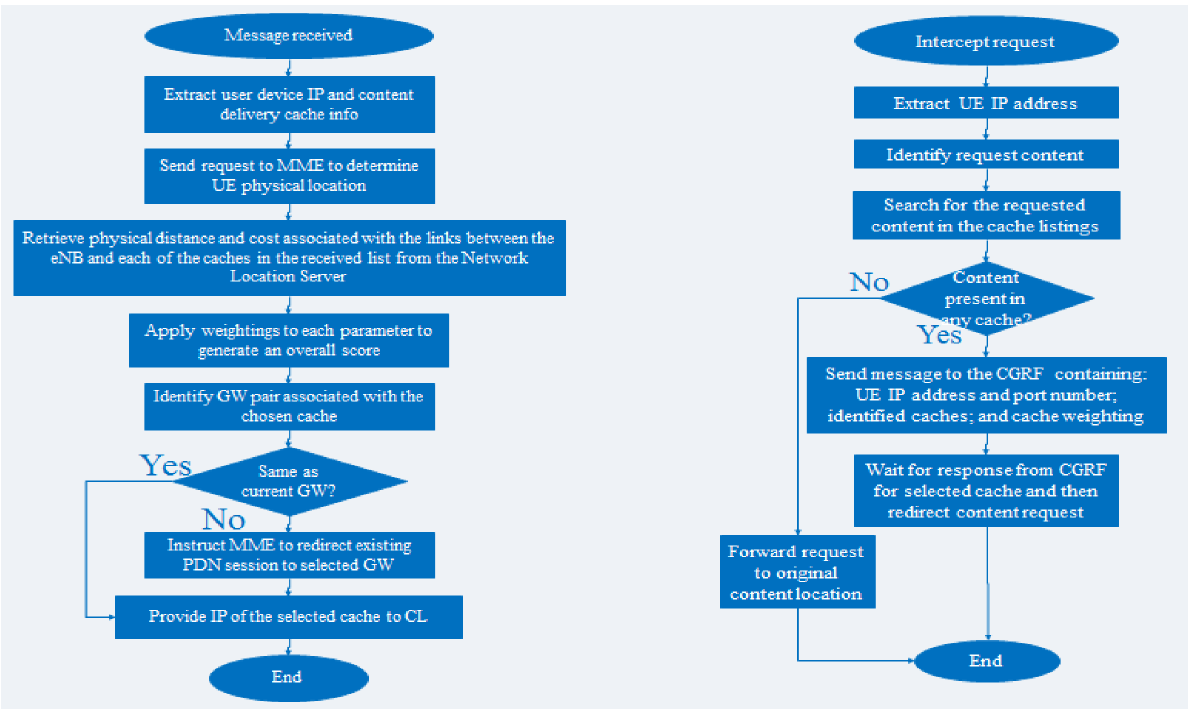


Figure 67 - CGRF algorithm & CL algorithm.

The process in which the CGRF associates a specific cost to the link between the subscribers to the different caches that hold the required content may take into account parameters like, distance, link speed, cache congestion, gateway congestion; and each one of those parameters can be assigned a different weight depending on the operator's policies and requirements.

Chapter 7: Infill

Covering densely populated areas has become easy, or easier, with the use of small cells and the cheap backhaul provided by fixed networks and the expansion of technologies like fibre [137]. But in rural areas it is more difficult to make it economically viable to improve coverage and capacity, as these are less densely populated and the return in investment is lower. The same can happen in isolated areas or difficult to reach environments used by some private enterprises (petrol extraction, mines, gas). Simultaneously, some of the public transports, where you can find an extremely high density of subscribers are not getting their coverage and bandwidth needs fulfilled [138] [139] [140](train, underground- see Figure 68, planes…), both because of the challenging radio conditions and/or the extremely high density of subscribers, in these circumstances what is offered is a substandard service that cannot be compared to fixed and mobile broadband offerings elsewhere. In these last cases, the problem is not delivering high capacity in a highly dense environment, but backhauling the connectivity in a moving mode of public transport.

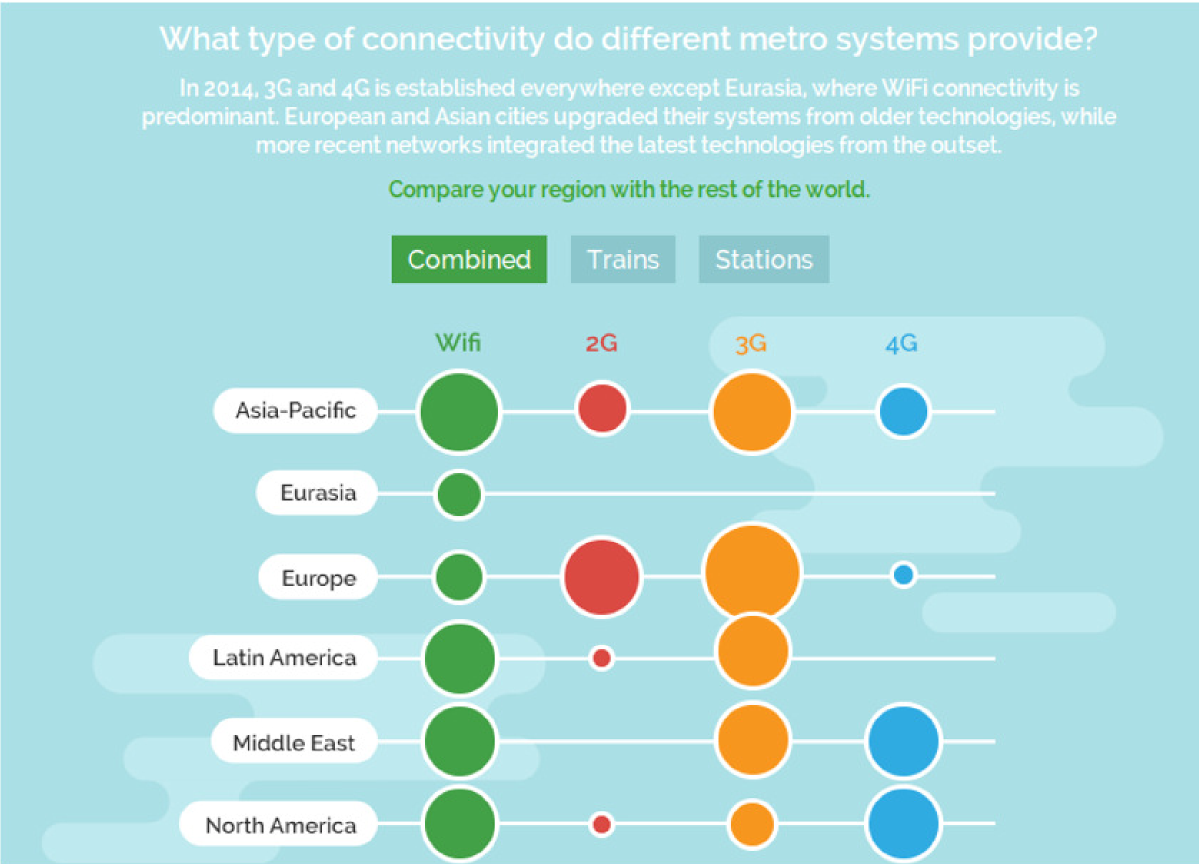


Figure 68 - Different underground connectivity solutions by continent (Source: newcitiesfoundation.org).

In order to move towards 5G, solutions to improve capacity and coverage in these “difficult” to deliver scenarios needs to be addressed to avoid having a huge gap in user experience compared to dense or “easy” to deploy offerings.

"Building a state of the art gigabit infrastructure, combining fibre based (including hybrid) and wireless networks to provide a high-speed Internet access for everyone and "every-thing" is one of the most important European projects of our time. But to fund an ubiquitous coverage is very difficult. Telecommunication companies, regulators and governments have to open up and challenge their long-established beliefs in order to achieve a breakthrough in closing the gap towards a gigabit society."- ***René Obermann*** *[141]**,** Chief Executive Officer, Deutsche Telekom.*

7.1.State of the Art (2012)

On rural areas broadband providers had to come up with new ways to deliver their services. ISPs (Internet Service Providers) tend to try to use wireless technology to avoid the long and costly cable deployments, for example:

- Sugarnet [142], using point to point technology to deliver broadband. Drawbacks: requires always antenna on roof, an expensive installation fee and more than average urban broadband monthly costs.
- Rural Broadband Parnetship [143], which tries to empower communities to run, manage their own rural broadband projects or help fund other ISPs to make it cost effective for them to deliver their services. It also provides examples of successful wireless and wired deployments. Drawbacks: requires extra funding quite often undertaken by the subscribers.
- UKBroadband [144], which is studied in more detail in Section 8.3. It uses 4G technology in the 3.6GHz or 5.8GHz band (Making necessary the use of external antenna on the roof) and requires an initial investment to deploy the base stations and the core equipment to cover an area, these costs need to be passed to subscribers in the form of an initial installation fee or more expensive monthly costs.

On Section 7.2 we propose a shared 4G network with a mobile operator to provide both fix wireless rural broadband and mobile services using the same infrastructure by two different operators. The result is a service that can be compared to urban wired broadband at a similar cost to the end user.

On urban areas there are several systems designed to deploy communications onto buses or trains [145] [146] [147]. There is also a growing passenger and operational demand for connectivity between aircraft and ground [148]. Currently this is being achieved on long haul flights using a satellite backhaul link but this solution is expensive [149], heavy and has a high delay (240-279ms in geostationary orbits). A terrestrial solution has many advantages but is only possible over land or within about 250 km of land. A terrestrial solution can provide a cost-effective, dedicated pan-European coverage.

BT is exploring development of a pan-European network of ground stations that provide connectivity to aircraft to enable passengers to have Wi-Fi access to the internet. This terrestrial system using wireless links from the aircraft direct to the ground is known as DA2GC (Digital Air-to-Ground Communications). Lufthansa, Deutsche Telekom [150] and Aero3G have proposed such systems, with BT supporting the last of these.

The present status of the discussions around spectrum bands for DA2GC is that ETSI have drafted System Reference Documents describing the technology, and passed these to CEPT (European Conference of Postal and Telecommunications Administrations) with a request to identify harmonised spectrum bands. CEPT ECC (Electronic Communications Committee) has established Project Team SE44 looking at the sharing and compatibility issues between DA2GC systems and other services operating in the candidate frequency bands, and Project Team FM48 (Spectrum Aspects Broadband DA2GC Systems [151]) to prepare a draft regulation for the operation of DA2GC. A number of spectrum bands have been studied but the 5.8 GHz band has emerged as the most promising candidate studied so far.

7.2.Rural Mobile Broadband over Shared LTE RAN

BT is committed to bringing the highest speed broadband possible to everyone in the UK. BT's commercial fibre broadband rollout plus innovative partnerships like Cornwall and the Isles of Scilly, Northern Ireland and others spurred on by BDUK funding could see >90% of UK premises have access to fibre broadband by early 2016 [152].

It is believed that just 2 per cent of UK premises will be deemed 'not spots' - receiving below 2 Mbps. This will make it hard for individuals and businesses to perform very basic tasks that the majority of the UK population is already taking for granted, let alone achieving multi-device usage in one building.

BT is seeking solutions for these premises. TV White Spaces, BET (Broadband Enabling Technology [153]) and satellite services may all play a role and this trial set out to test whether a shared LTE solution was a possible addition to that mix.

The initial task assigned was to design the tests that would determine the success or failure of this solution and capture the data (both from the network and trialist feedback).The objectives were:

- Prove a shared LTE radio access network can deliver a technically and commercially viable solution.
- Determine the customer experience on a loaded, live LTE network.
- Provide live trial performance results informing the UK broadband debate.

Since October 2011, the trial saw BT and Everything Everywhere collaborating to provide fixed wireless and mobile broadband to 180 customers living in and around St. Newlyn East in

Cornwall. From the start, the project was focussed around the key requirement to deliver an experience of at least 2 Mbps downstream to the all trialists, which in turn, would then allow them to use broadband applications and content. The radio access network and core network were carefully designed to facilitate this. In addition tests and network performance changes were made to the network during the trial with the aim of optimising customer experience:

1. Varying maximum upload/download speeds, see Section 7.2.1.1.
2. Selective use of external antennas, see Section 7.2.1.1.
3. Using of quality of service prioritisation, see Section 7.2.1.2.

A minimum of 4 Mbps download and 1 Mbps upload was provided with average speeds of 12-13 Mbps for download and 4-5 Mbps for upload. Trialists were able to enjoy TV on demand, HD video, VoIP, on-line back-up, photo sharing, online gaming and home working.

Most trialists valued a consistent and reliable service with low latency, with many saying they would pay more for this level of service. The trial also generated 86% engagement, a figure far higher than the average in these types of trials.

The trial saw up to 10 times more traffic from the fix trialist (BT) than the mobile trialists (EE), see Figure 69, where one of the KPI (Key Performance Indicator) used, eNB Downlink throughput shows the difference. This is due to the fact that up to 10 devices were connected per LTE hub compared to a single device for mobile dongle.

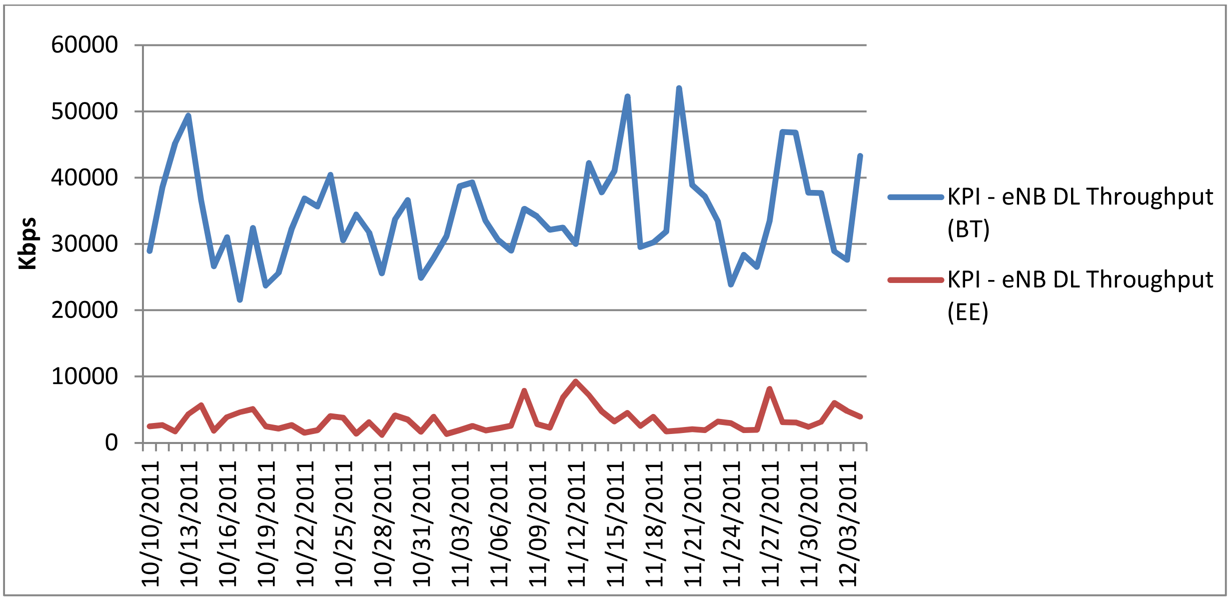


Figure 69 - eNB downlink capacity per operator (BT and EE) during the first 8 weeks of the trial.

7.2.1. Tests, Results and Feedback

Different tests were implemented during the trial months. These tests were designed to understand the capabilities of LTE as well as the effect of some network changes in the customer experience and in the balance of radio sharing with EE.

Both BT and EE had 80 trialists each surrounding the St. Newlyn East village, which was considered a no-spot for broadband and mobile data services coverage.

BT was giving their trialists a Wi-Fi hub (similar to BT Home Hub) that used LTE RAN as backhaul, mimicking a broadband deployment, while EE gave LTE USB (Universal Serial Bus) dongles to connect to their laptops to their trialists, trying to imitate a more mobile/nomadic subscriber. As we can see in Figure 70, the BT data usage is similar to the one expected in a fix broadband operator.

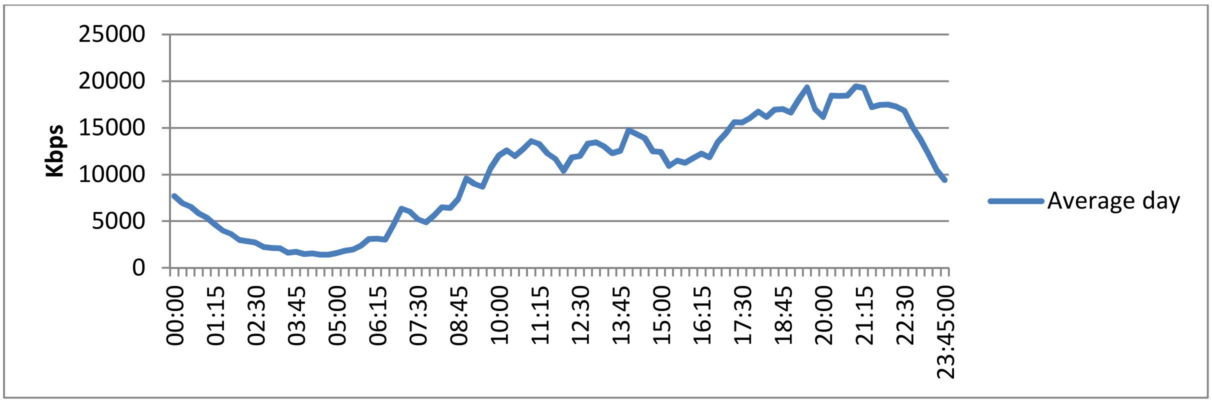


Figure 70 - BT average data usage day as seen by the BT EPC.

The users were distributed over the coverage area at an average distance of 3280 m from the eNBs, one eNB was placed just outside of Newquay (provided by NSN) and the other east of Mitchell (provided by Huawei). The division of BT trialists between the cells/sectors was then one shown in Figure 71:

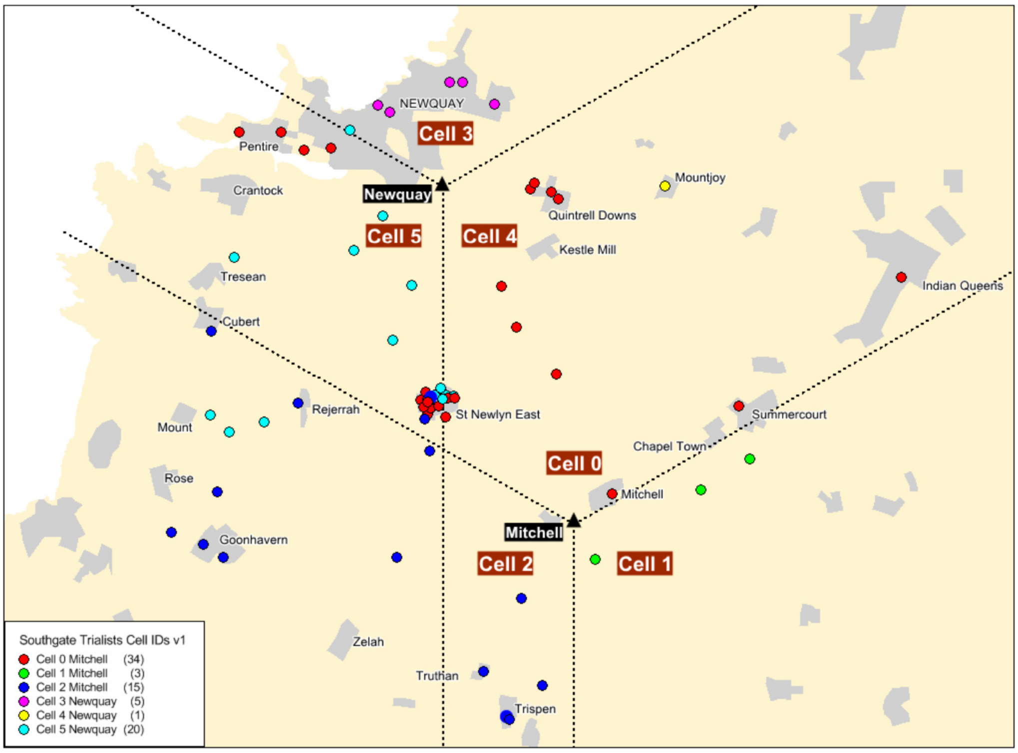


Figure 71 - Map of BT trialists location and eNB attachment. Mitchel-Huawei (sectors: 0, 1, 2), Newquay-NSN (sectors: 3,4,5).

The reason for the difference in number of subscribers between Mitchel and Newquay eNBs was due to the height of the antenna. Newquay was a reused tower from EE in an urban/suburban area (with height restrictions), while Mitchel was a BT rural tower with full height.

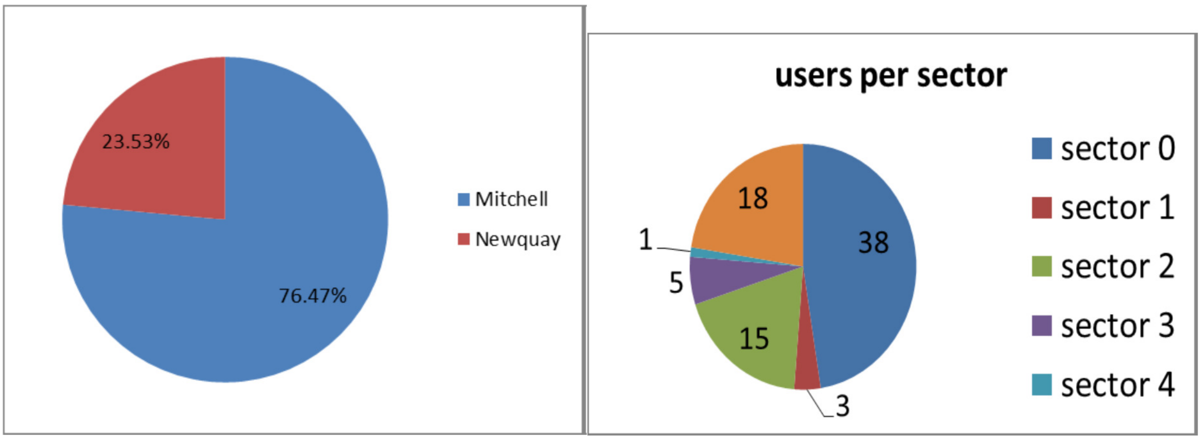


Figure 72 – BT users per eNB and per sector.

Both BT and EE had sector 0 as the most loaded (~60 users between them), and sector 0 has been considered during the trial as the most realistic sector, see Figure 72, and the one to be used to extract any conclusion on user experience and network loading.

Although all these tests where done independently from the tests done by EE, the idea was to prove 2 operators could work independently and use the same RAN, all the tests and roll-back mechanisms had to be agreed and demonstrated in the test network before deploying in the live one, in case any of the proposed tests started to affect the other operator's trialists' performance.

7.2.1.1. Speed Caps and Speed Tests

All speeds recorded by trialists were taken using speedtest.net, averaged during the same day at 3 different times.

8 Mbps Speed Cap

To get a level of confidence in the network stability, especially in the interaction between fix mobile broadband users and mobile users, the trialists speeds were capped at 8 Mbps for 4 weeks (for EE trialist capped at 4 Mbps). These were the results during that initial phase:

- At installation time taken by engineer 8 Mbps cap (network not loaded), see Table 15.

Table 15 - 8 Mbps speed cap at installation time.

	DL speed (Mbps)	UL speed (Mbps)	% of users that did the speed test
average	7.19	3.57	100.00%
max	15.00*	10.09	
min	1.69	0.08	
average sector 0	7.40	2.87	89.47%
max sector 0	13.00	9.40	
min sector 0	1.70	0.35	

*As network not yet fully loaded sometimes the speed test was able to go over the 8 Mbps over the first 2s of the connection.

- 8 Mbps cap after 4 weeks of the network running (network loaded), see Table 16.

Table 16 - 8 Mbps speed cap with fully loaded network.

	DL speed (Mbps)	UL speed (Mbps)	% of users that did the speed test
average	5.96	3.99	81.48%
max	15.31	11.61	
min	1.20	0.11	
average sector 0	4.67	2.86	68.42%
max sector 0	8.04	9.56	
min sector 0	1.20	2.86	

We can see that the variability is quite high already; during later stages of the trial one of the aims was to make the experience more consistent across all trialists.

After face to face interviews with the trialists it was discovered that most preferred a constant speed instead of high peaks at idle times. At the end of the trial we left the trialists again at 8 Mbps for 4 weeks. At this point with the changes that had been made in the network, as a result of this study and optimizations, over 80% of the BT trialists achieved between 8-6 Mbps download speeds.

16 Mbps Speed Cap

After the 4 initial weeks at 8 Mbps the speed cap was put at 16 Mbps. The trialists were asked to inform us of their speeds with this new limit, see Table 17:

Table 17 - 16 Mbps speed cap with fully loaded network.

	DL speed (Mbps)	UL speed (Mbps)	% of users that did the speed test
average	9.65	5.06	64.20%
max	19.23	15.50	
min	0.22	0.22	
average sector 0	8.05	4.20	47.37%
max sector 0	16.06	13.56	
min sector 0	0.22	0.28	

We can see that average speeds increased; although it also meant that trialists with worse radio conditions got an even worse result. This is due to how the eNB scheduler assigns bandwidth trying to give more to users with better radio conditions so they can complete their tasks and allow more bandwidth for slower users. In this case, because the users with good radio conditions are allowed more bandwidth and they congest the node leaving very little bandwidth available for subscribers with bad coverage.

Unlimited (no caps in uplink or downlink)

All the caps were removed just before Christmas, see Table 18:

Table 18 - Unlimited speeds (no cap in upload or download).

	DL speed (Mbps)	UL speed (Mbps)	% of users that did the speed test
average	11.91	4.85	40.74%
max	26.52	15.98	
min	2.35	0.26	
average sector 0	9.02	4.77	50.00%
max sector 0	20.16	11.26	
min sector 0	2.36*	1.63	

* Value higher than in the 16 Mbps speed cap because the specific trialist with the lowest speed in the 16 mbps test did not reply to the feedback request for the unlimited speed cap. This customer was at a later stage installed with an external antenna and his speeds increased to over 10 Mbps.

With the caps removed the downlink results (Figure 73):

- 79.41% of the trialists got over 6 Mbps.
- 58.82% of the trialists got over 8 Mbps.

With the caps removed the uplink results:

- 79.41% of the trialists got over 2Mbps
- 44.12% of the trialists got over 4Mbps

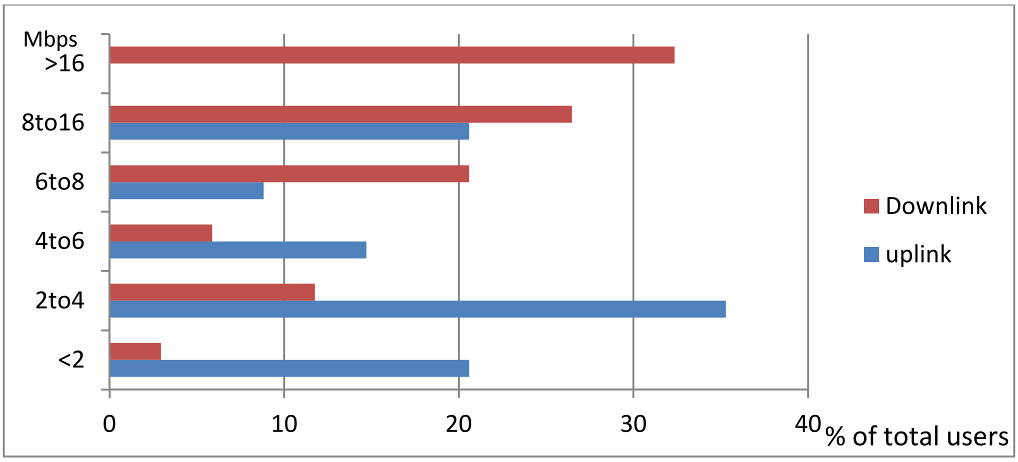


Figure 73 - Downlink and Uplink speed test without any cap.

Other Learnings

Most of the users were told to use the LTE hubs with the internal antennas they came with, but to some users with low signal at installation point we offered an external dipole antenna that attached at the back of the hub with a gain of 2 dBi. Finally, to users with very low signal and far away from the eNBs, we offered external antennas with 9 dBi gain that were mounted to the eves of the house (~ 3 m high).

Table 19 - Average distance to eNB and average speed for the different types of antenna.

	Total number	Average distance to eNB (m)	Average downlink (Mbps)	Average uplink (Mbps)
External antenna	4	5681	13.34	5.01
Dipole antenna	7	3122	12.98	2.50
No antenna	22	3110	10.89	5.31

In Table 19, high average downlink on external antennas suggests that some potential participants that were rejected participation on the trial, because in the initial analysis it was considered they were too far away for an acceptable service (no external antennas considered), could actually have been used as part of the trial if an external antenna had been supplied. Also in Table 19, the lower uplink in the dipole antenna is caused by the fact that when using a dipole antenna the MIMO capability is lost and it has a higher impact on the uplink; the same happens with external antennas but this is counteracted by a much higher antenna gain. No antenna was installed in subscribers that had a good enough connection (3 bars or more)

Because of the use of different antennas depending on the radio situation of each trialist, most trialists had a good signal level that allowed high speeds. When looking at the users' performance, it does not seem to correlate hugely to distance to the eNB (Figure 74), but more to the congestion in the sector they are placed (Figure 75), this suggests that the use of the correct antenna type can equalize the distance to eNB between trialists.

See Figure 74, where we can see first that because of the use of external antennas distance does not seem to be the discriminating factor.

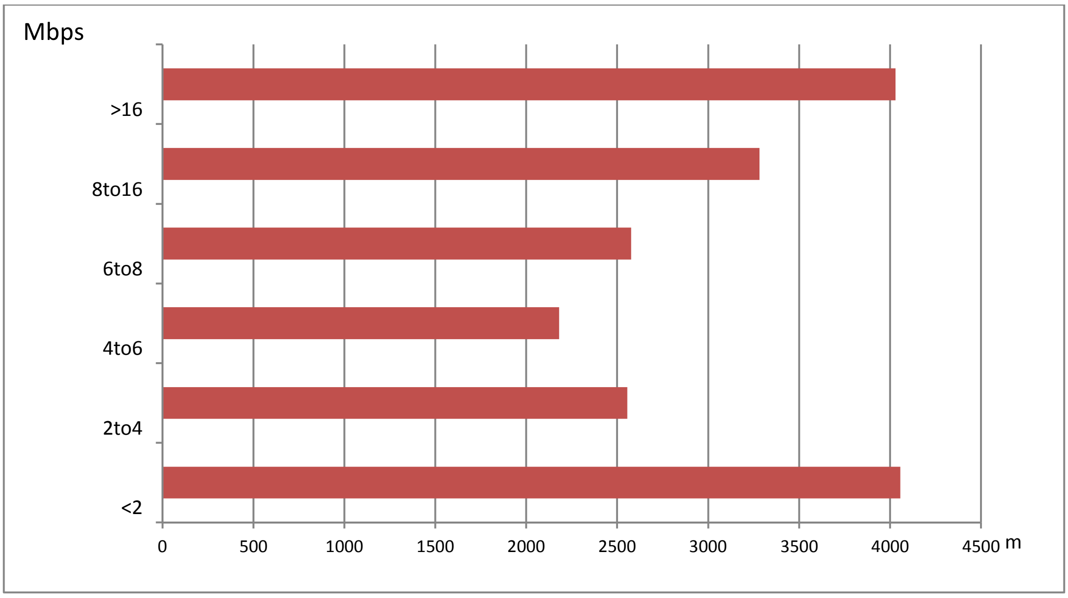


Figure 74 - Average distance to eNB (m) vs downlink speed (Mbps).

On the other hand, see Figure 75, where the most congested sector, sector 0, is the one with lower uplink and downlink speed.

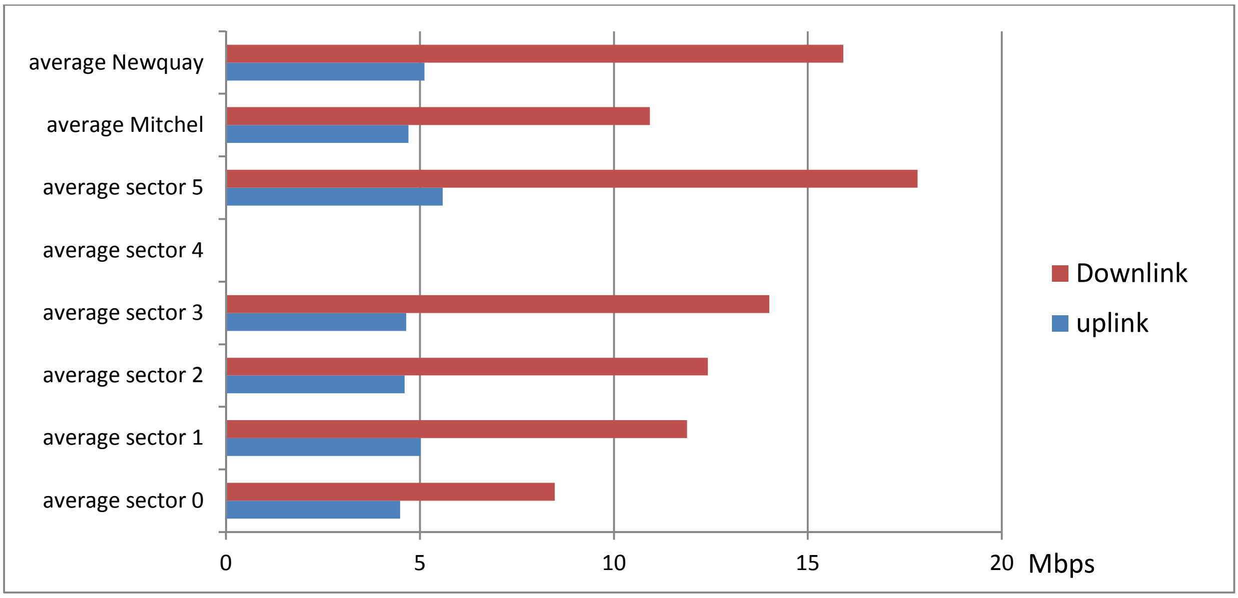


Figure 75 - Average speed in each of the different sectors.
Note: The single user in sector 4 didn't reply to this test.

The above calculations leads to believing that in a fix mobile broadband scenario where the operator can make sure that each user regardless of distance to eNB has a good enough signal, applying the adequate antenna depending on the customer situation, the main factor affecting user experience will be congestion caused by the number of subscribers in the sector. Ways to improve congestion would be:

- Decrease the power of the congested sector to decrease its coverage while increasing the power of other nearby sectors to try to change which sector some of these congested subscribers connect to.
- Use directive antennas to force some subscribers to connect to a different sector.
- Reduce the maximum speed limit to increase the available capacity resources.
- Add more frequencies in the area. Needs more spectrum and more equipment.
- Consider this congested area for improvement of the broadband technology used if economically viable.

External Antenna Placements

Only 10 external antennas were initially placed for the trial to trialists far away from the eNBs. Later, after the second set of speed tests was reported by the trialists, 5 extra antennas were deployed for users with low performance mainly due to the fact of being in a hard to reach location (from radio perspective, see Figure 76).

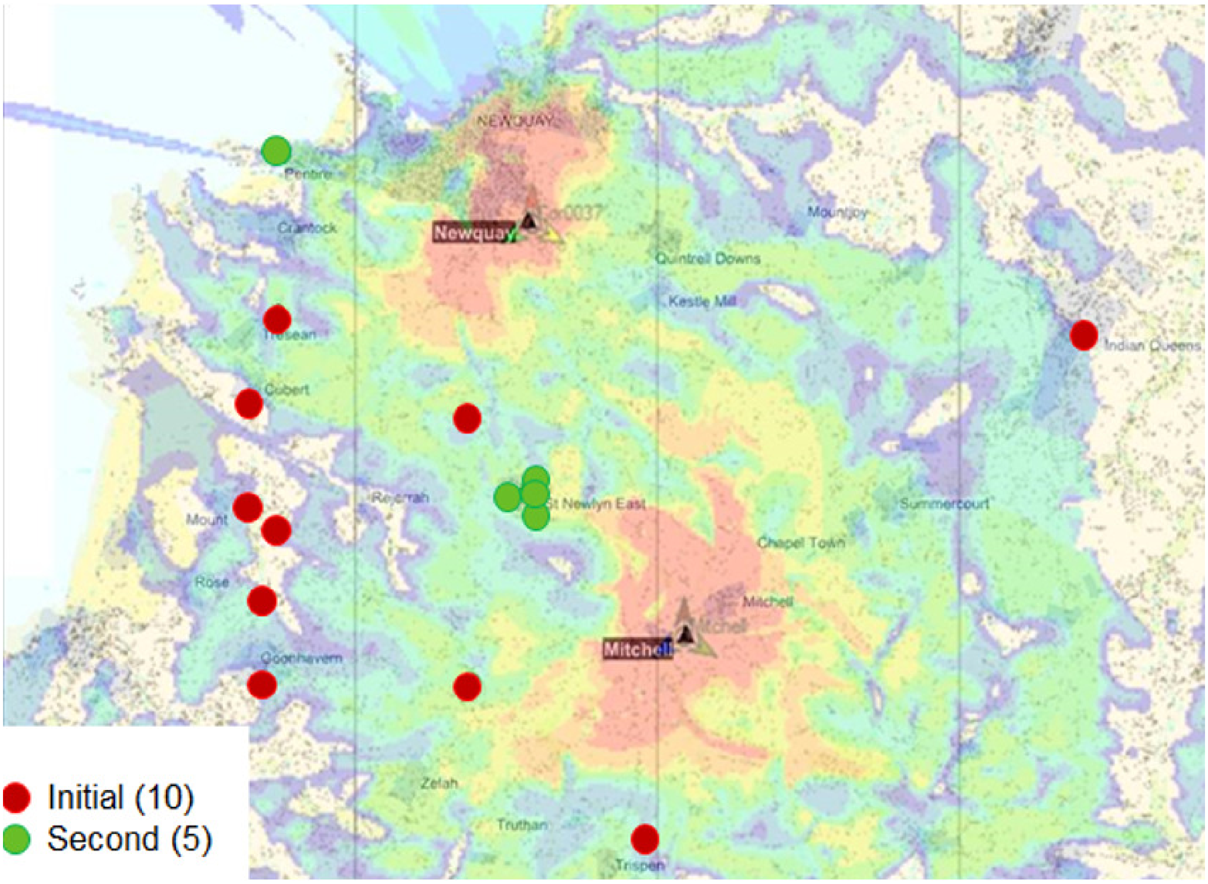


Figure 76 - Location of external antennas.

7.2.1.2. Prioritization

After the initial tests looking at performance with the speed caps it was decided to test prioritization of traffic, first prioritization specific traffic types and then prioritization traffic from different users depending on their current level of service to try to level the UX..

Dedicated Bearer Test

End users from sector 0 (most loaded sector) were asked to watch 2 videos, one delivered over dedicated bearer (with QoS activated) and another with default bearer (best effort). There was only 45% participation, which is not a bad trial engagement, but we only had 29 users on sector 0, making the results of this test inconclusive.

70% of the trialists that participated were doing other things while watching the videos. This does not mean that the person doing the test was doing something else, but that there were more devices/users connected to the same LTE hub that were using the network. If we take the results from these customers as a more congested situation, we obtained a worse mark from them for the dedicated bearer, but the difference in the average times a video stopped increased from 31.5% in the dedicated bearer test to 33.5% in the best effort test. In theory, as more congestion was added the more difference between the experiences of both videos will appear.

This test was not completely successful because although user experience barely changed from the responses to the questionnaires there was certain improvement observed from the EPC point of view. Also the congestion when performing the test was not high enough for the end users to notice the difference between the dedicated bearer and default bearer delivered videos, and the number of participants was too low to have a reliable data output. To improve the test procedure more subscribers need to be recruited and an artificial source of congestion added. This can be done with 5 laptops controlled by the testers initiating massive downloads during the test time.

From the monitoring that was in place while the test was being done by the trialists, we can see that the network did not change its performance dramatically while they were performing this test so we can take out network issues as a differentiator of the video performance.

Gold/Silver/Bronze Test

With this test the objective was to increase the speed of those customers with lower speeds by giving priority to their traffic over the rest, this was done by assigning different QCI (QoS Class Identifiers) to the different trialists, see Table 20. These QCI were defined by 3GPP thinking on the minimum needs of different services run over the network.

Table 20 - 3GPP defined QCI table for LTE (source 3GPP)

QCI	GBR type	Priority	Delay budget (ms)	Packet loss rate	Example services
1	GBR	2	100	10^{-2}	Conversational voice
2	GBR	4	150	10^{-3}	Conversational video (live streaming)
3	GBR	5	300	10^{-6}	Non-conversational video (buffered streaming)
4	GBR	3	50	10^{-3}	Real time gaming
5	Non-GBR	1	100	10^{-6}	IMS signalling
6	Non-GBR	7	100	10^{-3}	Voice, video (live streaming), interactive gaming
7	Non-GBR	6	300	10^{-6}	Video (buffered streaming)
8	Non-GBR	8	300	10^{-6}	TCP-based (e.g. WWW, e-mail) chat, FTP, p2p file sharing, progressive video, etc.
9	Non-GBR	9	300	10^{-6}	

The test was performed in the Huawei eNB for 2 reasons:

- The Huawei eNB offered throughput protection to EE trialists (a vendor specific feature) and EE insisted on this to protect their trialists' user experience.
- The Huawei eNB had a higher level of congestion as 75% of trialists were within its coverage and the test would yield more meaningful results in a congested network.

3 different types of user were defined, Gold (QCI7), Silver (QCI8) and Bronze (QCI9). These 3 QCI were chosen because they don't offer a better packet loss or delay over the best effort service (QCI9) and only packet prioritization is performed (See Table 20).

Users were assigned to each group depending on their speeds but also some users from higher speeds and good engagement on the trial were added to Gold and Silver groups to see the difference in higher speed users.

As a result of this test, the average speed of the users went down but Gold users with low speeds (under 4 Mbps) got an average improvement of 0.7 Mbps. In sector 0, the most loaded sector during the trial, the improvements were greater against the results of silver and bronze users. Sector 0 gold members that were under 4 Mbps went from an average of 2.66 Mbps to 5.62 Mbps.

This result shows that prioritization only makes sense and can be noticed in highly loaded cells, and in these cases, in a fixed mobile broadband proposition, it could be used as a tool to improve the speeds of the users that have worse radio conditions.

7.2.1.3. Automatic Speed Tests

Because of the decreasing participation on the requested tests from trialist, in March 2012 automatic speed test robots were placed in several points of interest under the trial coverage, these robots did a speed test every 30 min and recorded upload/download speed, delay, jitter and packet loss. These robots were extremely useful to collect a constant stream of data from the trial user experience, and in hindsight, it would have been useful to have them installed from the beginning of the trial.

The locations chosen were ones where BT could securely store a laptop or PC connected to an LTE hub via Ethernet cable. The locations were (see Figure 77):

- Newquay robot: placed in the Newquay BT exchange, with good coverage from the Newquay eNB.
- Crantock robot: placed the Crantock BT exchange, in theory in an area without coverage 8.8 km from eNB, but in a third floor with an external antenna.
- Trerice robot: placed in Trerice House from the National Trust, sitting in between the coverage of sectors from different eNBs. In exchange, a second LTE hub was provided to this site for the use of Trerice House National Trust administrators.
- Mitchell robot: placed in the Mitchell BT exchange, in close proximity to the Mitchell eNB.

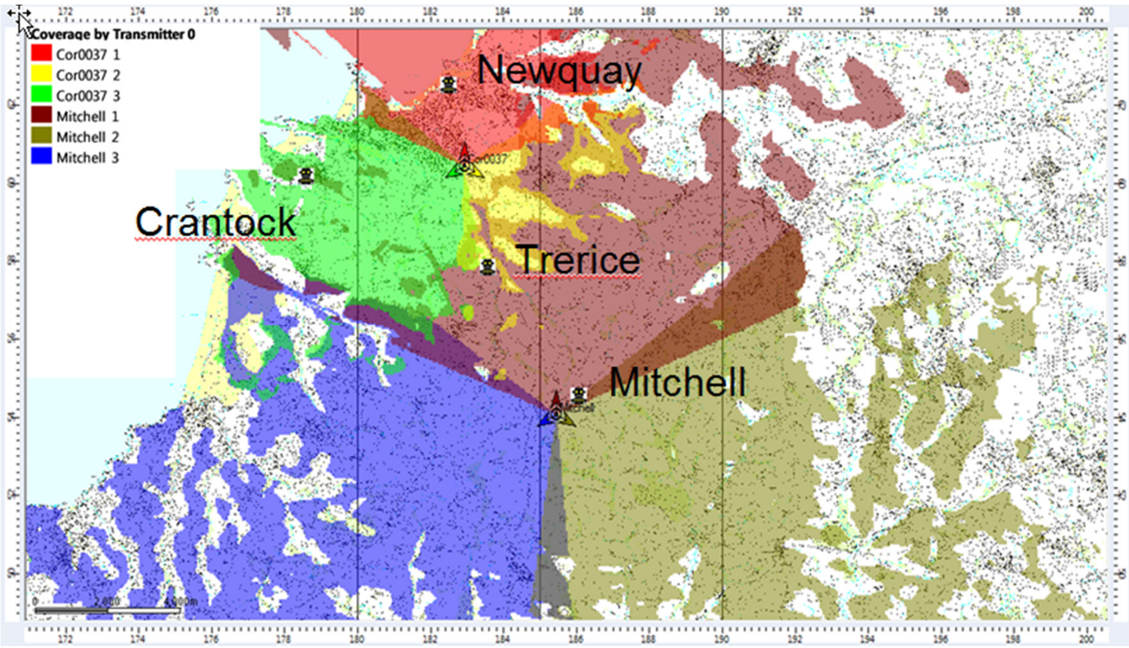


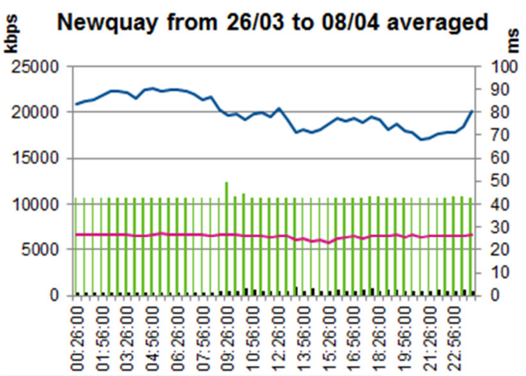
Figure 77 - Location of test robots and coverage map of the different sectors.

At the same time when this test was devised by BT, EE decided to join and a second laptop with a dongle attached to it was placed in each of the locations except Mitchell.

The software used to collect this information was JD Automatic Speed Tester [154].

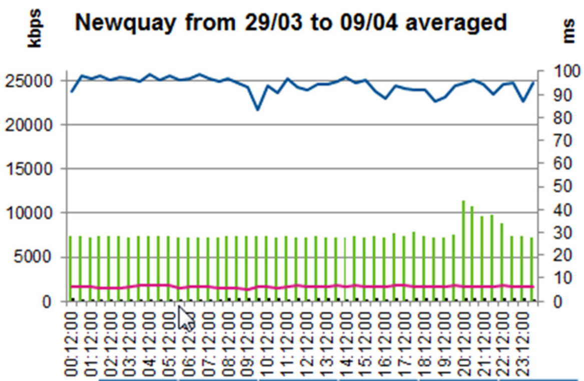
In Figure 78 below, we can see how time of day affects the peak speeds achievable in Newquay.

BT



	DL kbps	UL kbps	Delay ms	PKL%	Jitter ms
AVG	19906	6503	43	0	2
MAX	22586	6780	50	0	4
MIN	17004	5767	43	0	1

EE

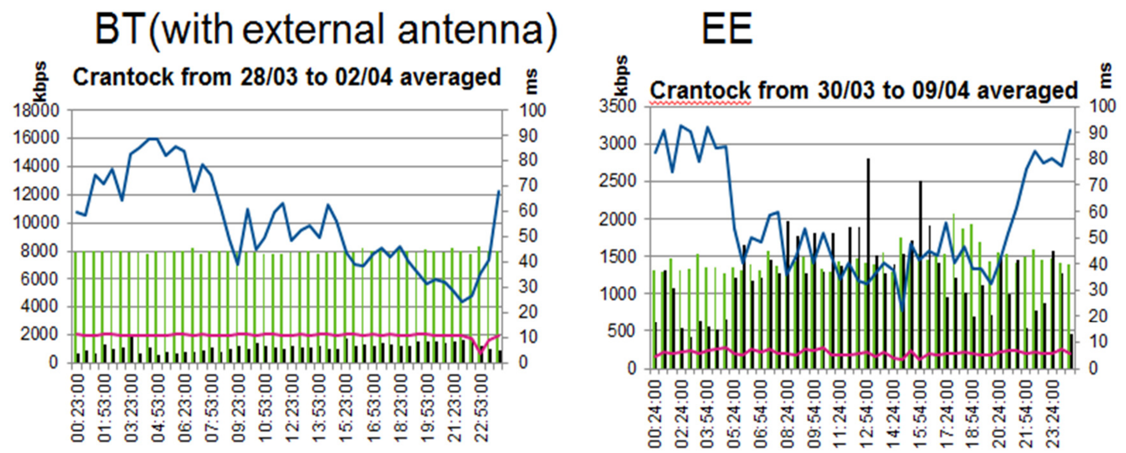


	DL kbps	UL kbps	Delay ms	PKL%	Jitter ms
AVG	24499	1650	29	0	1
MAX	25671	1819	44	0	2
MIN	21679	1363	28	0	1

Figure 78 - Newquay robot results from BT and EE. Results taken every 30 min averaged over a week.

Newquay robot was placed in the Newquay exchange and it was very close to the Newquay eNB, for this reason speeds were not affected by time of day as the Newquay eNB was not very loaded. Also the EE LTE dongle was placed in a different room from BT LTE hub, one floor higher. Differences on the delay are explained by the close proximity of EE EPC core in Bristol and the more complicated and longer trip data had to do to get to the BT EPC core in Ipswich.

The robot in Crantock exchange was placed far away of the Huawei eNB in sector 0, the most highly-loaded sector in the trial.



BT (with external antenna):

	DL kbps	UL kbps	Delay ms	PKL%	Jitter ms
AVG	10023	1961	44	0	6
MAX	15980	2024	46	0	11
MIN	4370	666	43	0	3

EE:

	DL kbps	UL kbps	Delay ms	PKL%	Jitter ms
AVG	1967	208	42	0	36
MAX	3250	277	59	1	80
MIN	785	121	37	0	12

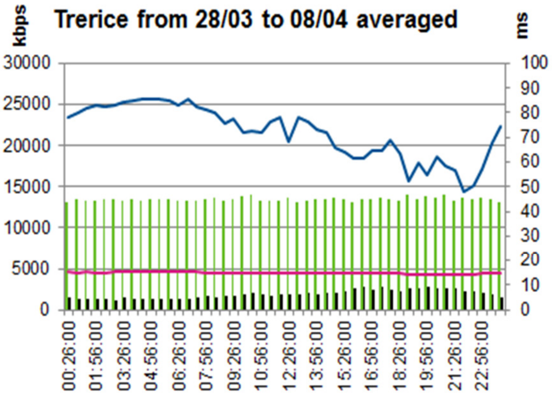
Figure 79 - Crantock results from BT and EE. Results taken every 30 min averaged over a week.

The EE dongle in Crantock is unable to obtain high data rates because of the distance, while the BT LTE hub can get some adequate performance only because of the external antenna installed in this location (they are connected to an eNB 8.8km away), see Figure 79. The EE jitter and delay data show that the radio channel is not ideal, nevertheless a minimum of nearly 1 Mbps download and 120kbps upload is achieved which is way better than 3G at those distances in a loaded cell.

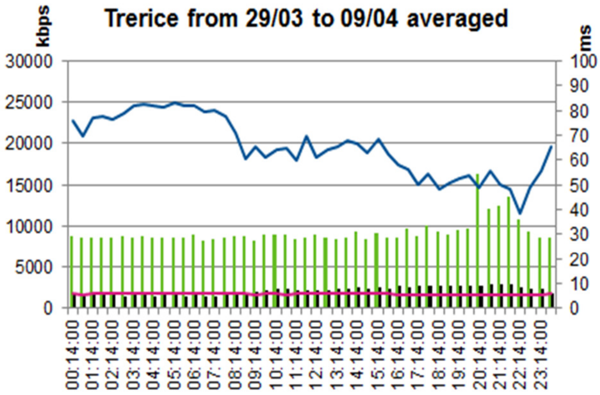
The robot in Trerice is located very close to the main no-spot targeted by this trial, also within the sector 0, most congested.

BT and EE download speeds are perfectly matched in Trerice, see Figure 80, and the effects of congestion clearly visible. Although the BT delay is 10-12 ms more, the jitter follows the same pattern in both, showing that the busy times for both operators coincide. Again because of the antenna separation on the hub, uplink throughput in the BT hub is twice the EE dongle.

BT



EE



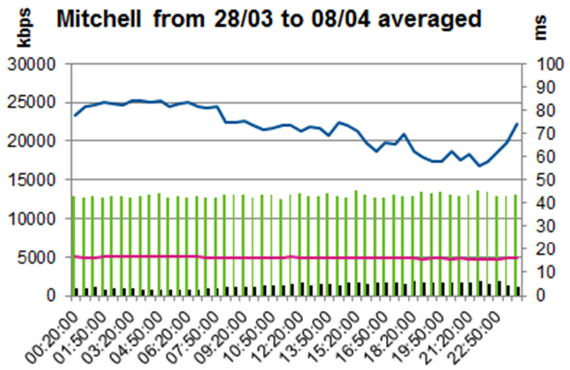
	DL kbps	UL kbps	Delay ms	PKL%	Jitter ms
AVG	21605	4456	45	0	6
MAX	25680	4600	47	0	10
MIN	14452	4241	44	0	4

	DL kbps	UL kbps	Delay ms	PKL%	Jitter ms
AVG	19624	1712	31	0	7
MAX	24894	1794	55	0	10
MIN	11477	1576	28	0	5

Figure 80 - Trerice House robot results during a day averaged over a week.

In Mitchell only BT placed a robot.

BT



EE

No EE robot in Mitchell Exchange

	DL kbps	UL kbps	Delay ms	PKL%	Jitter ms
AVG	21726	4877	43	0	4
MAX	25262	5006	46	0	6
MIN	16784	4644	42	0	2

Figure 81 - Mitchel robot results during a day averaged over a week.

BT hub in Mitchell exchange follows a very similar pattern to BT and EE in Trerice, see Figure 80 and Figure 81, and this was the reason EE decide not to put a robot in this location.

In May all users were capped again to 8 Mbps to check if that would give a more consistent experience during all day, a smaller difference between the achievable speeds at peak and idle times. As the robots where already in place doing speed tests every 30 minutes, there was no need to ask the trialist to do speed tests.

7.2.1.4. Other Testing

During the trial, other testing with Ofcom and the BBC was also performed.

Ofcom

BT advised Ofcom that from our testing DTTV (Digital Terrestrial Television) interference had been observed at Adastral Park. Ofcom was supplied with a LTE hub for Out of Band Emission test performed by RF (Radio Frequency) Industries Ltd and Ofcom was supported on Out of Band Emission technical queries and practical measurements. These tests were completed in Adastral during 1st-2nd December and during the 15th December on the live Cornwall Network.

BBC (British Broadcasting Corporation)

The ability for BBC to stream live SD (Standard Definition) and HD broadcast content was demonstrated on the live trial network. The BBC was interested in Outside Broadcast Opportunities created by LTE as currently they use a unit that requires 7 to 8 3G SIMs and has a cost of £30.000, while with LTE they could achieve a similar performance with one single SIM and a ruggedized portable unit under £2000.

Comments by Colin Muir (BBC Technology Project Coordinator): “Our group recently viewed the original recordings and we're particularly excited about the fact that they were broadcast over a single access point, as well as the fact that we managed to broadcast a simultaneous live audio feed during our motion tests. This opens up a number of opportunities for us and could potentially enable us to broadcast live radio and TV coverage over a single mobile access point/vehicle - something we'd like to explore with you further”

7.2.2. Summary

LTE can deliver rural broadband no spot infill solution but it will require careful wireless planning.

A single radio access network can be shared effectively between an MNO and a fixed operator reducing the cost and risk of deployment and operation. The dual EPC model works, both BT and EE’s EPCs have been working without issues, even when faults happen in one of the EPCs the trialists of the other operator remained unaffected. Resources can be shared fairly between the MNO and the fixed operator. To share effectively between the two operators a tight control over the subscribers speeds and allowances is required from the HSS or PCRF, moreover a fair usage policy in the eNBs can guarantee that there will always be enough bandwidth for any of the two operators subscribers. This last policy in the eNBs gives an extra level of freedom to both operators as it means that no matter what polices the put their subscribers if within coverage will be served, in congestion cases the policy will move guarantee 50% of resources for each operator.

The maximum number of fixed users that can be deployed per site is ~200 counting mobile and fixed users (estimation from the number of users in sector 0).

Self-install will only work for people that don't require external antenna. External antenna is probably needed for people over 4.5 km. The end user gets high enough speeds and low delay/jitter for any of the current applications broadband users are accustomed to.

7.3.Danube: Wi-Fi Access on Board Planes via 3G TDD Backhaul

BT partnered with Aero3G to test the user experience delivered by the Aero3G DA2GC in the 5.8GHz band which used UMTS (Universal Mobile Telecommunications System) TDD aka TD WCDMA. At the time of this partnership BT was engaging to gauge interest with several airlines, and one of the more interested ones was EasyJet. It was decided that, to make the user experience test as realistic as possible, it had to be done in an aircraft with the real 5.8GHz UMTS TDD backhaul in place. The plane couldn't leave ground as most of the equipment we wanted to use hadn't been certified for aircraft use yet.

At the same time, a review the Aero3G system and their claims of expected usable throughput at different heights situations was done. Aero3G provided the results and logs from a real flight test they performed in conjunction with GDB (General Dynamics Broadband).

After this successful test and verification, the author was in charge of providing the technical data for the SOR (Statement of Requirement) for the avionic equipment including the UMTS TDD modem.

7.3.1. DA2GC User Experience Trial with EasyJet

By using a standard commercial plane, the level of service received by the passengers could be measured. The trial had to be designed to deliver the best user experience within the cabin with a limited backhaul (up to 10 Mbps). To maximize the user experience and improve the perceived downlink capacity it was decided:

- That a small cache in the plane containing the most viewed content would reduce the backhaul utilization. A 5TB (Terabytes) cache was selected for its small size and functionality. This server could cache predefined content and dynamically requested content.
- A content server on board would provide movies/music on demand for which the users wouldn't need any type of backhaul.
- A login page was created to welcome passengers to the service and steer them towards the content server.

The plane cabin could have up to 180 users with at least 1 device per user; although statistically, and from BT marketing research information, only up to 30% of users would be using the service simultaneously in a full flight. Because of this, a decision was made to try both 3 APs with 5 GHz and 2.4 GHz and 5 APs with 2.4 GHz and 5 GHz (although only 3 had 2.4 GHz radio turned on to limit co-channel interference), see Figure 82. The selected APs also had a feature that delayed the response on 2.4 GHz attachment requests, effectively steering the 5 GHz capable devices to 5 GHz, leaving the congested 2.4 GHz spectrum freer for exclusively 2.4 GHz only devices.

Weight is one of the main concerns for airlines as it increases the use of fuel, therefore the APs used needed to be powered via PoE to reduce the weight of 65 m of power line cabling.

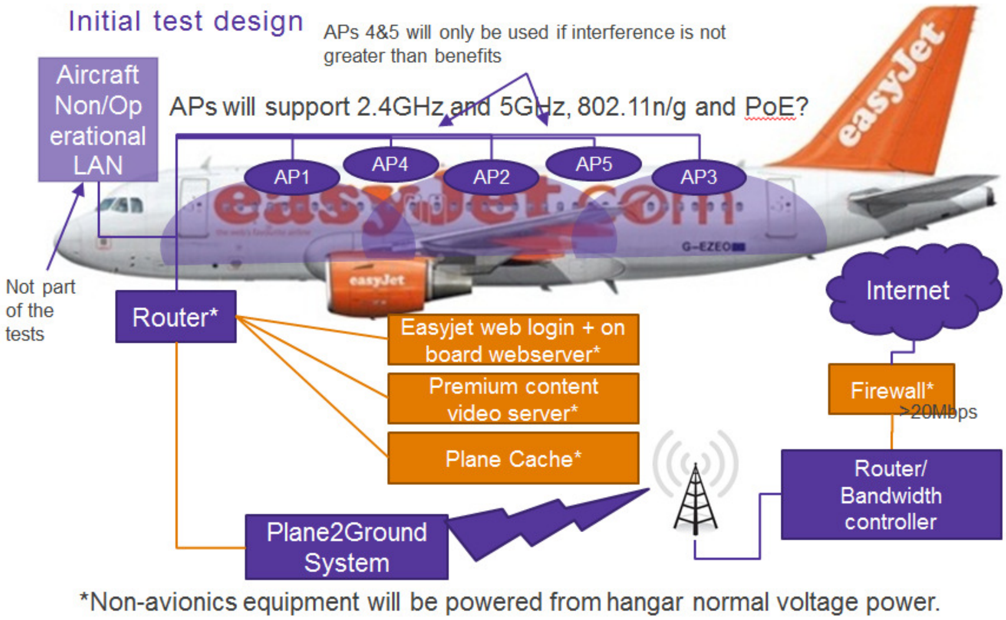


Figure 82 - EasyJet trial design.

EasyJet allowed the use of an airplane (Airbus A319) for 5 days divided in 2 visits 2 weeks apart. This type of plane has a capacity of 156 seats (26 meters by 4.5 meters).

During the first visit, the author was allowed to get on board and install temporarily all the equipment to measure performance. EasyJet allowed to conceal the Wi-Fi APs behind the plane main cabin ceiling as this would be the most likely location for installation and the radiation pattern would be closer to reality. The attenuation of the panels (ceiling boards that cover the visible ceiling from inside the cabin and allow access to internal hull of the aircraft) was measured as 2dB (Figure 83).

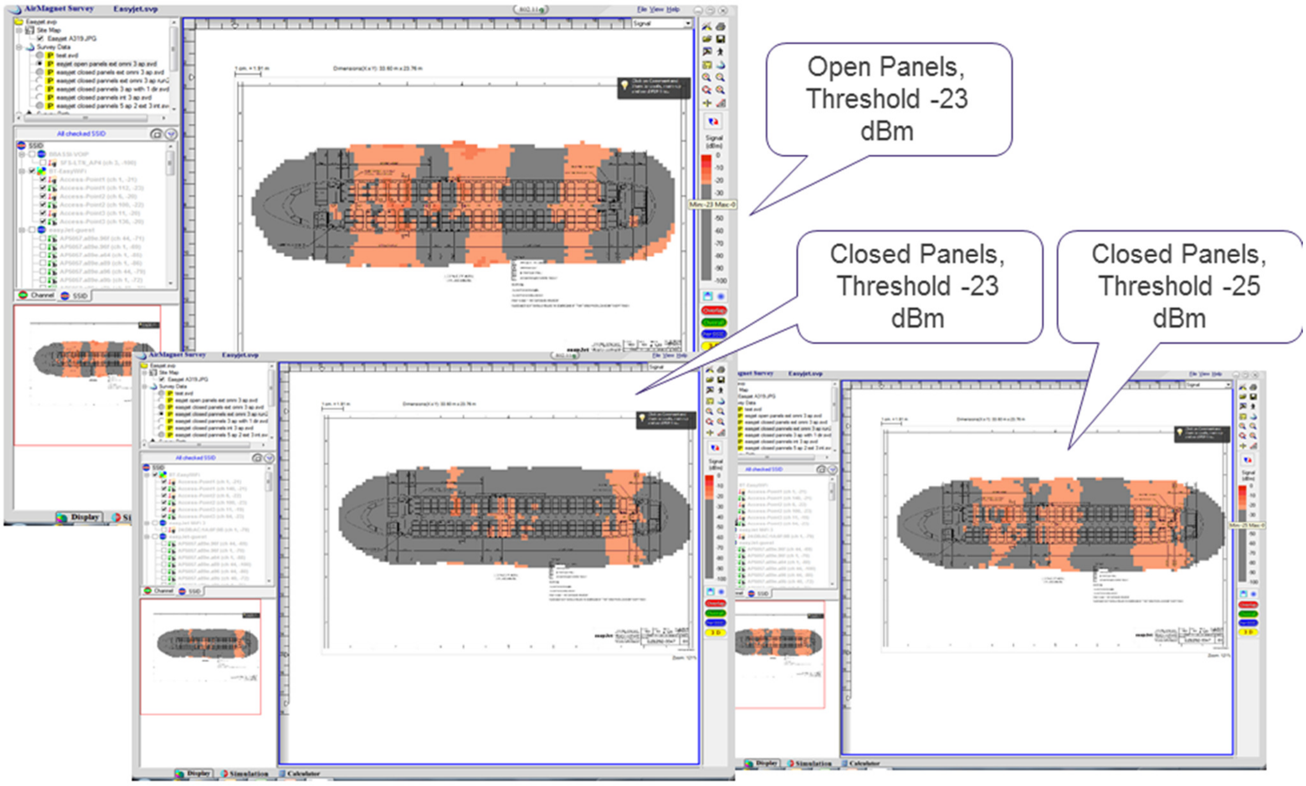


Figure 83 - Panel attenuation calculation.

Open panel: when the panel has been removed.

Closed Panel: when the panel is in place.

The threshold level allows us to view how the radiation is spread.

The tests were performed both with internal omnidirectional antennas and external omnidirectional antennas (both with a 3dB gain) and surprisingly the internal omnidirectional antennas showed a better coverage in the tests (possibly due to the external antenna orientations used). So internal antennas usage was selected for ease of installation, weight reduction and simplicity (Figure 84 and Figure 85).

An initial Wi-Fi coverage map was created using this architecture, we tried initially with just 3 access points radiating both at 5GHz and 2.4GHz with just 20dBm EIRP (Equivalent Isotropically Radiated Power) and for the map a threshold of -33dBm (which is still considered a good enough signal for Wi-Fi) was used (see Figure 84 and Figure 85). Lower than -33dBM could still get a connection but can't be guaranteed an optimum speed.

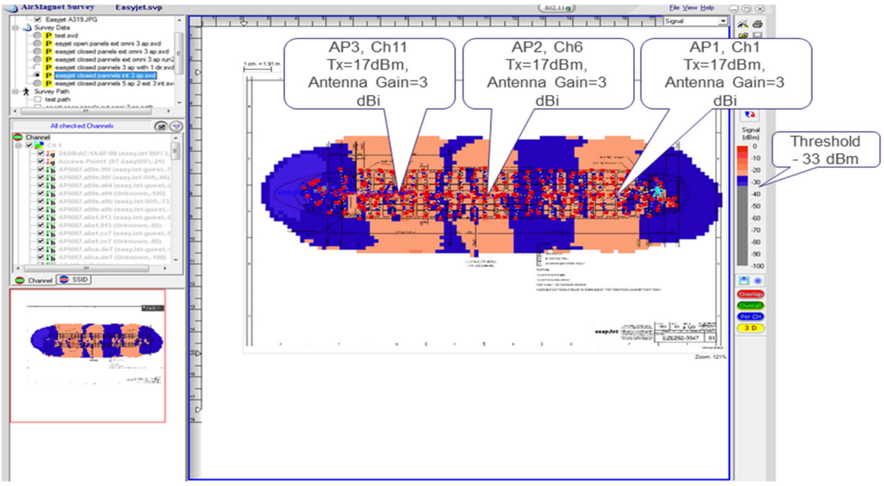


Figure 84 - Coverage with external omnidirectional antennas.

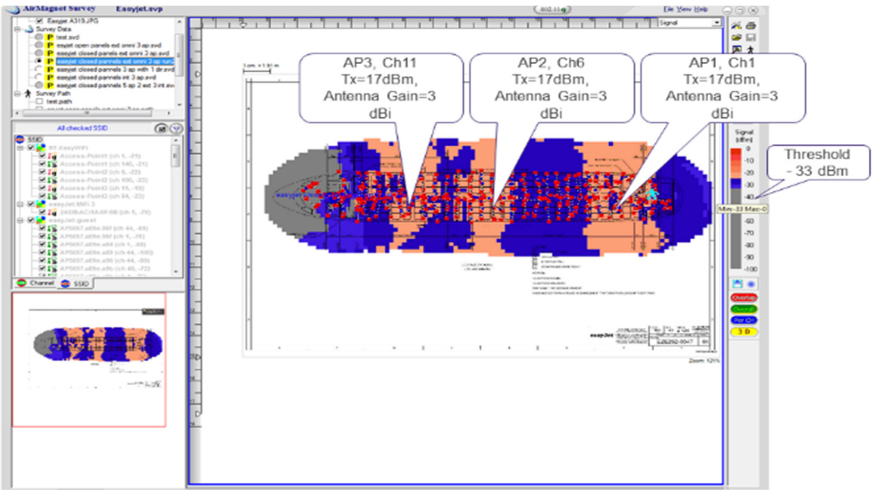


Figure 85 - Coverage with internal omnidirectional antennas.

From the map in Figure 86, it is clear that coverage is not an issue as there are no interferers (same is expected in flight).

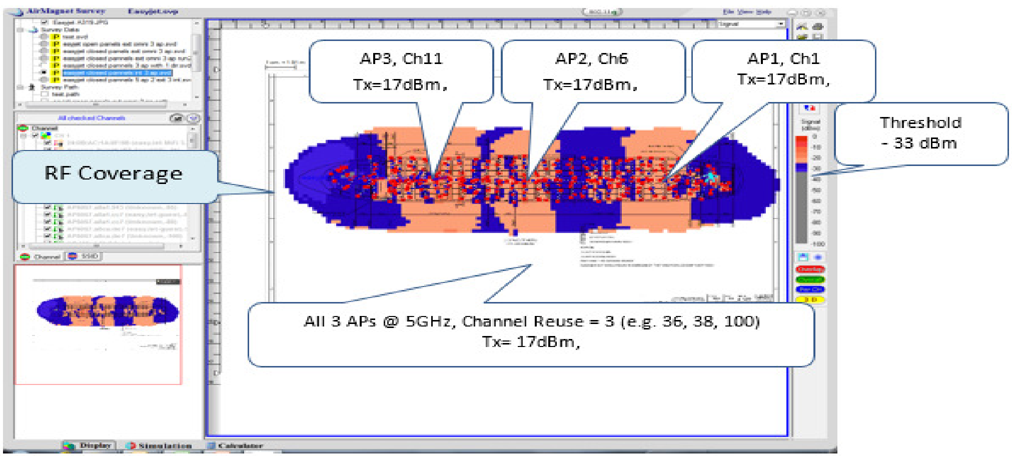


Figure 86 - Coverage map with 3 APs at 2.4 GHz and 5 GHz.

The main issue would be to provide enough bandwidth to each passenger, so it was decided that installing 2 more 5 GHz APs would increase the user experience for all the users. And this was the setup that was used for trialling with EasyJet employees on the following visit.

On this first visit also the UMTS TDD system (aircraft modem with antenna and UMTS TDD base station connected to a broadband line) was tested and its signal lowered to the expected power and throughput for an aircraft on cruising altitude. The main reason for this test was not to probe the UMTS TDD technology worked but to find the best Wi-Fi setup/design to provide an excellent service to passengers.

Figure 87 - From left to right: lifting the ceiling panels to place the APs; Boeing 747 used for trial/tests; Main cabin ceiling void.

On the second visit, all the equipment was installed behind the ceiling panels in the main cabin as in the initial test (see Figure 83 and Figure 87), and several EasyJet senior people were invited to take part in the trial where several tasks needed to be completed.

In the case of a fully loaded plane (150 people) AP3 would have had a maximum of around 30 people connected to it – in the test it had 31 people connected simultaneously, see Figure 88, which means that even in the worst case scenario the maximum load produced would be able to be supported with the current Wi-Fi architecture.

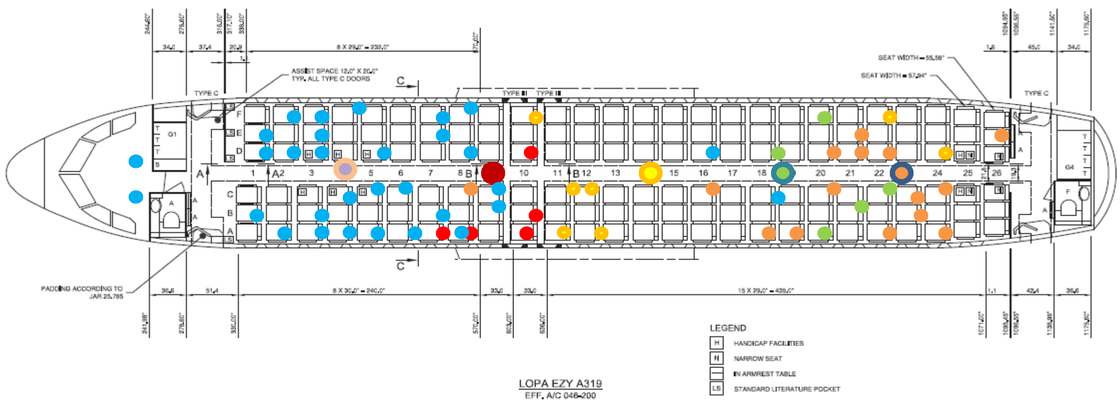
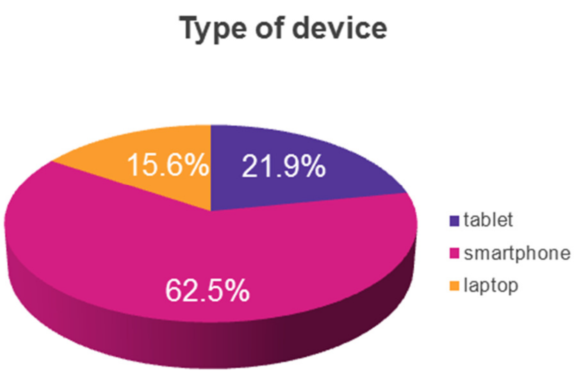


Figure 88 - Passenger location and colour of the AP they were associated with.

The "passengers" were asked to bring their own devices (Figure 89), they were divided in two teams and do 10 tasks (see Table 21) that were expected a user would perform in a flight having this type of service (browsing, watching a movie, listen to music, read the news, check email…) and afterwards they were asked to complete a questionnaire to assess the performance. See Annex D for the trialist brief and test description.

Table 21 - Test description for onboard Wi-Fi.

	Team 1	Team 2
Test 1	Turn on Wifi, select EasyWifi and login	Turn on Wifi, select EasyWifi and login.
Test 2	Click on the Easyjet banner and book a ticket.	Watch one of the cached videos.
Test 3	Download a file (116 MB).	Download a file (116 MB).
Test 4	Watch one of the cached videos.	Speed tests using speedtest.net.
Test 5	Connect to www.bbc.co.uk/news and browse (BBC is pre-cached).	Connect to www.bbc.co.uk/news and browse (BBC is pre-cached).
Test 6	Connect to www.thetimes.co.uk And browse (The Times is not pre-cached, cached progressively).	Connect to www.guardian.co.uk and browse (The Guardian will not be cached).
Test 7	Connect to cache and watch videos http://easycache.com/mirror/	Connect to cache and watch videos http://easycache.com/mirror/
Test 8	Free internet/app usage, except VoIP and video streaming.	Continue watching videos.
Test 9	Free internet/app usage, including VoIP and video streaming.	Continue watching videos.
Test 10	Free access	



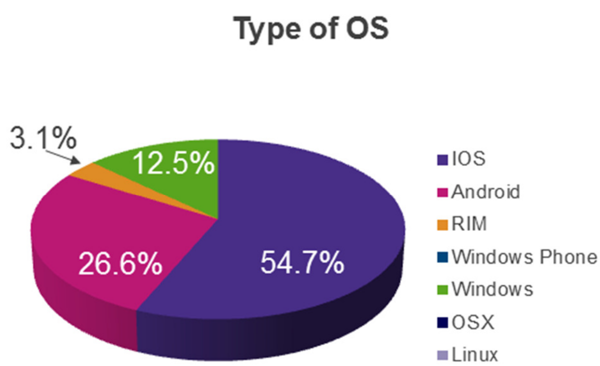


Figure 89 - Type of device and operating system used during the tasks.

From the results in Figure 90 and Figure 91, it can be seen that the performance is higher in the 5GHz APs as these are less congested and that the most congested APs have got a lower mark. The most congested AP is AP3 which has a 45% of the subscribers, see Figure 93, but only the 2.4GHz seems congested with 29% of participants (23 of them). The AP2 at 5GHz scores can't be taken into account as only 1 user connected to it.

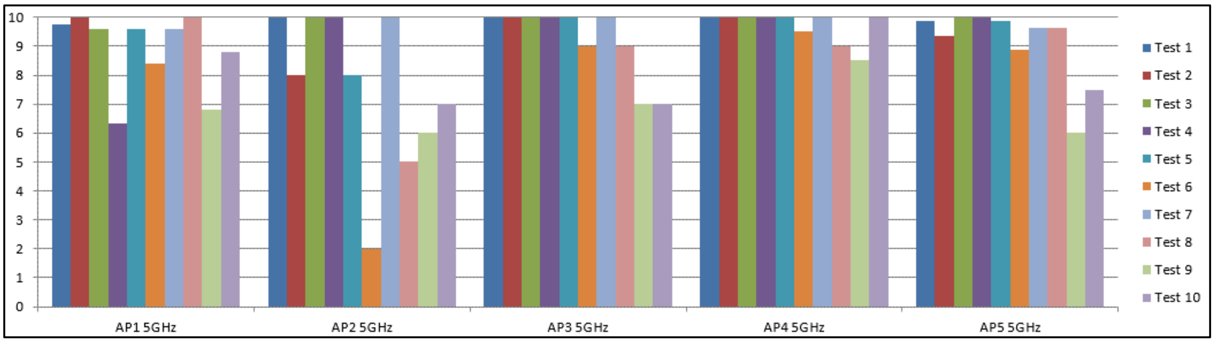


Figure 90 - 5GHz User perception markings of 10 tasks.

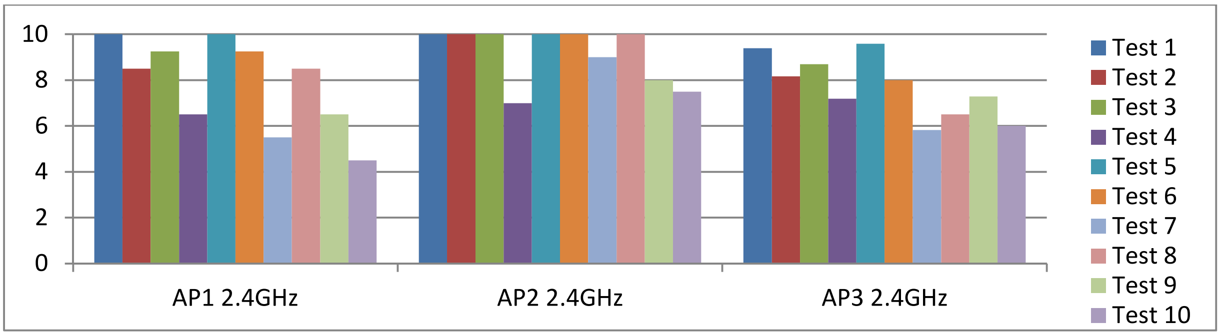


Figure 91 - 2.4GHz User perception markings of 10 tasks.

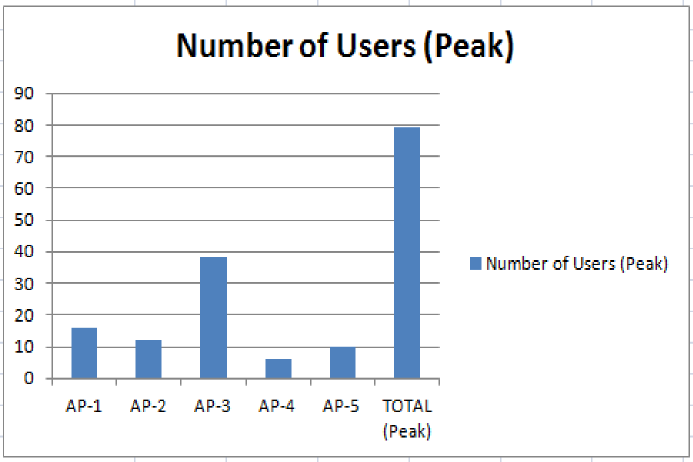


Figure 92 - Users per AP.

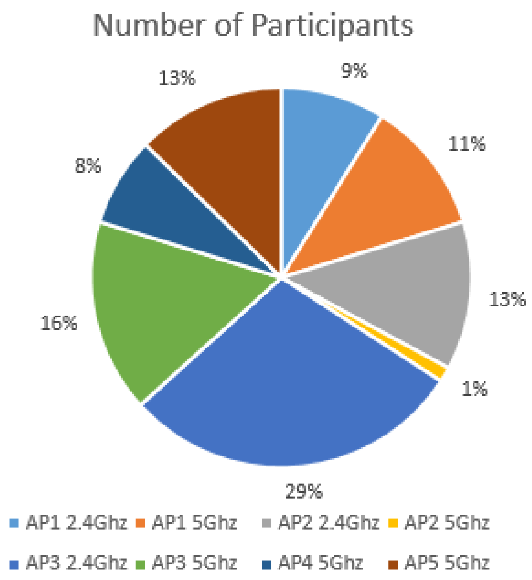


Figure 93- Number of participants in on board Wi-Fi test.

A total of 12.7 GB were used during 23 min by the 79 testers, see Figure 92. The peak IP data measured was 133 Mbps (when testing the video server). The peak throughput usage on the backhaul was 15 Mbps.

7.2.1.1. Summary

Some of the learning from these tests was:

- 5 APs with only 3 enabled for 2.4GHz and 5 for 5GHz provide the maximum bandwidth per user with the minimum interference (as the 2.4GHz APs can each use one of the 3 non-interfering channels) with a good compromise in weight.
- The cache interacted with speednet.net giving an overly optimistic result (over 40 Mbps).
- The cache needs to have a DNS built in otherwise the requests take too long to find the correct IP and this can alienate passengers.
- A decision needs to be made on whether voice and video conferencing over IP (VoIP and VVoIP) should be allowed as this can swamp the network. Initial testing suggests it would decrease the overall performance, and EasyJet feedback was that conferencing could also be an annoyance to other customers.

7.3.2. Aero3G System Verification

The reason why Aero3G decided that BT would be their partner of choice was because of the extensive knowledge in Wi-Fi networks and the large fibre European network with many PoPs (Point of Presence) which could be reused to host the ground base stations providing them with connectivity.

By clever usage of different antenna types (Omnidirectional, sectorial and directional), the main european routes can be covered with just 207 base stations in 33 countries (Figure 94) using 20 MHz of spectrum (5.855-5.875 GHz) [155]. The directional antenna at the basestation has a gain of 24 dBi and could reach a maximum of 180 km from the base station.

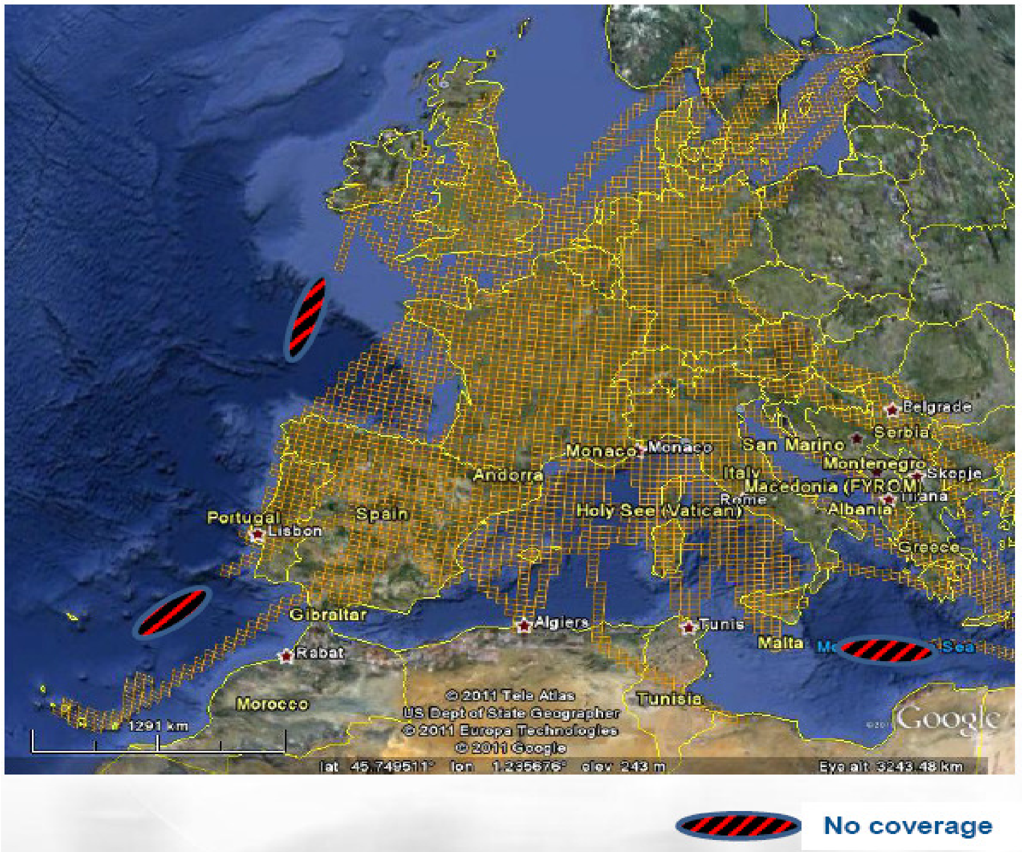


Figure 94 - Coverage of main European routes by Danube project (Source: Danube).

The Ground antenna consists of 6 sectors, 5 with a 72 degree horizontal beamwidth slightly elevated by 8 degrees surrounding a vertical antenna (Figure 95).

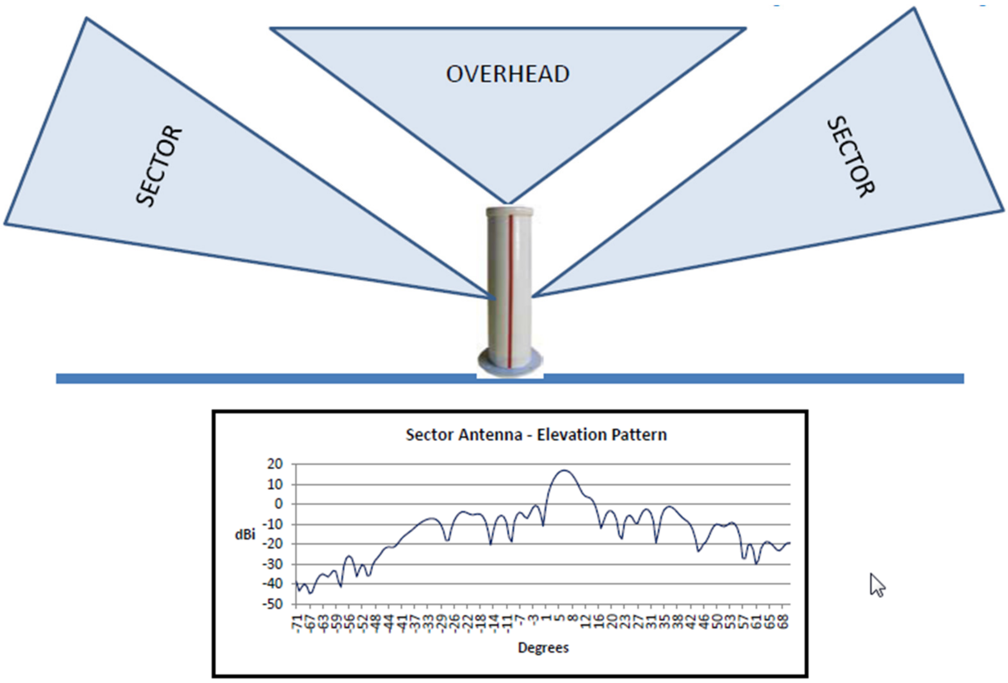


Figure 95 - Ground station antenna.

The Aero3G system uses a lot of air flight (speed, route, location,..) data to predict when each subscribed airplane is going to be covered by the different radios in the base stations and turn them on/off and use different inter-cell interference mitigation techniques to reduce interference (Figure 96).

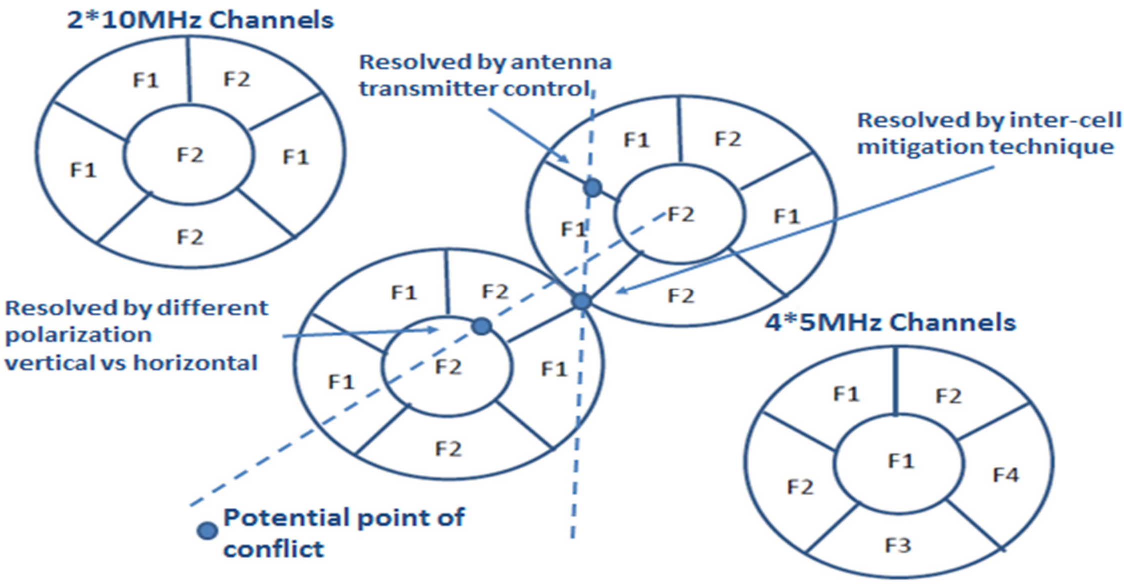


Figure 96 - Different spectrum usage and point of conflict resolution.

With these techniques Aero3G claimed (Figure 97) a better than 10 Mbps connection 80% of the time at cruising height (30000 feet) and a worse than 2 Mbps no more than 25% of the time at 10000 feet (which is the switch on cut-off point for Wi-Fi connectivity for passengers).

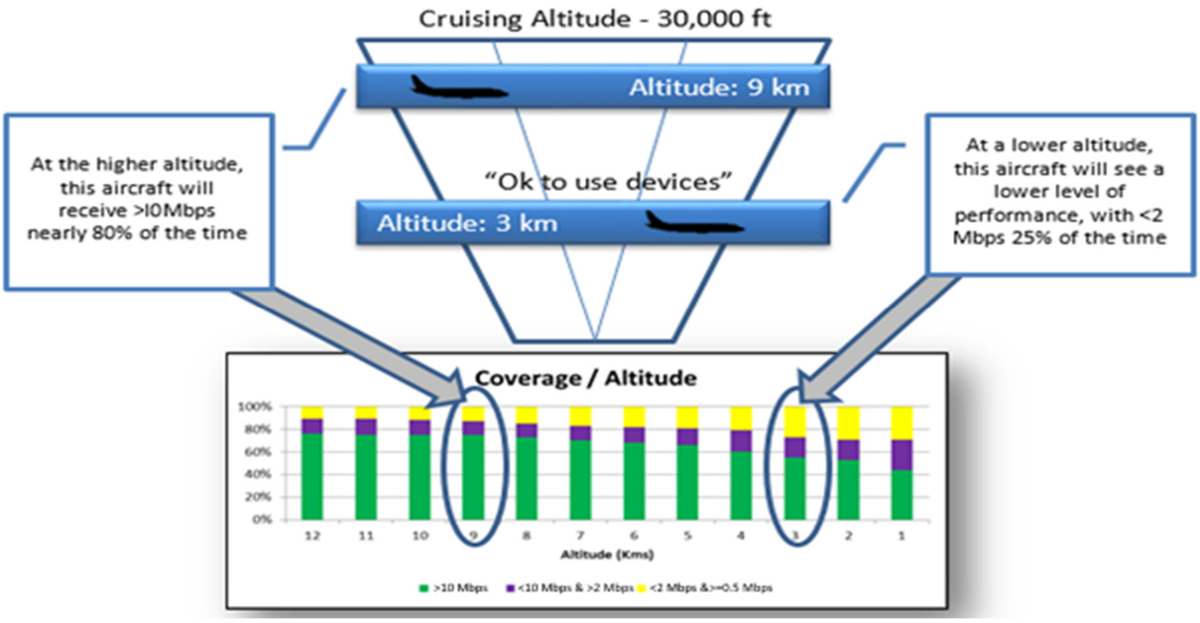


Figure 97 - Expected performance supplied by Aero3G.

Using the data supplied by Aero3G (which was also used in [156] [157]). A path loss model was then built and used the GBD UMTS TDD base station data to calculate maximum throughputs in different altitudes and distances.

UPLINK	plane2ground	Distance	120	km	120.33	DOWNLINK	ground2plane
		Bandwidth	10	MHz	7.68		
		Frequency	5865	MHz			
		Flight height	9000	m			
		Downlink slots	8	per frame	2		
		Basestation height	30	m			

UPLINK

	EIRP	39.00	dBm
From plane	power transmitted	36.00	dBm
	transmitter antenna gain	7.00	dB
	feeder losses	4.00	dB
	LINK MARGIN	3.66	dB
From basestation	Rx sensitivity	-103.00	dBm
	effective input power	-99.34	dBm
	receiver antenna gain	15.00	dB
	feeder loss	2.00	dB
	INTERFERENCE	-102.00	dBm
	Intracell	0.00	dB
	Intercell	0.00	dB
	Noise	-102.00	dBm
	Noise Figure	2.00	dB
	Max uplink badwidth	1.81	Mbps

PROPAGATION

PROPAGATION LOSS	151.34	dB
% of clouds/rain in path	10.0%	
100% Cloud fading	0.24	dB
rain fading in rain cell	0.1575	dB/km
100% Rain Fading	18.95	dB
Path Loss	149.42	dB
Rain intensity	30	mm/h

LINK ACHIEVABLE

Maximum speed achievable is calculated using Shannon's law taking into account the number of slots used backed off by a constant alpha below	
Alpha	0.90

DOWNLINK

	EIRP	51.00	dBm
From basestation	power transmitted	38.00	dBm
	type of antenna	SECTOR	
	transmitter antenna gain	15.00	dB
	feeder losses	2.00	dB
	LINK MARGIN	5.66	dB
From plane	Rx sensitivity	-103.00	dBm
	effective input power	-97.34	dBm
	receiver antenna gain	7.00	dB
	feeder loss	4.00	dB
	INTERFERENCE	-102.00	dBm
	Intracell	0.00	dB
	Intercell	0.00	dB
	Noise	-102.00	dBm
	Noise Figure	2.00	dB
	Max downlink bandwidth	9.46	Mbps

Slight rain:	Less than 0.5 mm per hour.
Moderate rain:	Greater than 0.5 mm per hour, but less than 4.0 mm per hour.
Heavy rain:	Greater than 4 mm per hour, but less than 8 mm per hour.
Very heavy rain:	Greater than 8 mm per hour.
Slight shower:	Less than 2 mm per hour.
Moderate shower:	Greater than 2 mm, but less than 10 mm per hour..
Heavy shower:	Greater than 10 mm per hour, but less than 50 mm per hour.
Violent shower:	Greater than 50 mm per hour.

Figure 98 - Customizable spreadsheet to calculate path loss and available throughput.

The Alpha value in Figure 98 was deducted from data provided by Aero3G on their flight tests using the equipment provided by GBD.

These calculations gave an expected throughput that verified Aero3G claims, see Figure 99, Figure 100 and Figure 101:

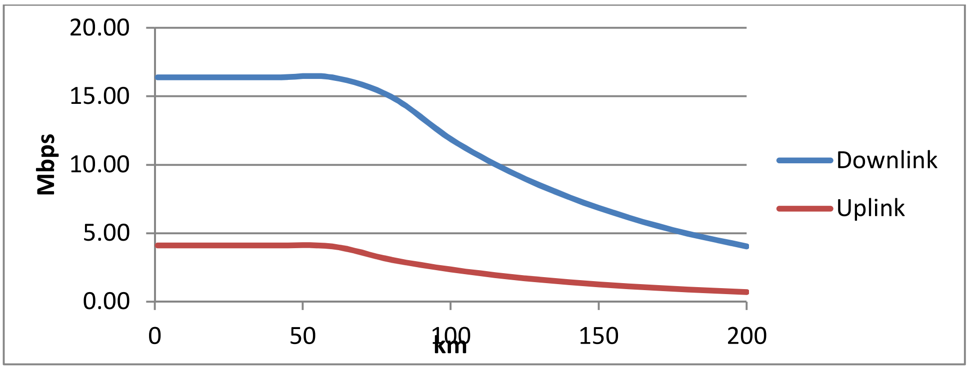


Figure 99 - Expected results with sector antenna.

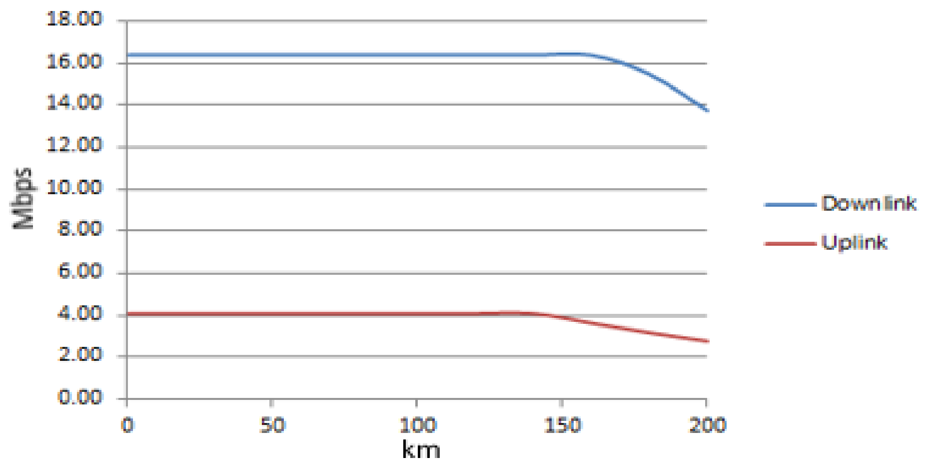


Figure 100 - Expected performance with directional antenna, for over-the-sea connectivity.

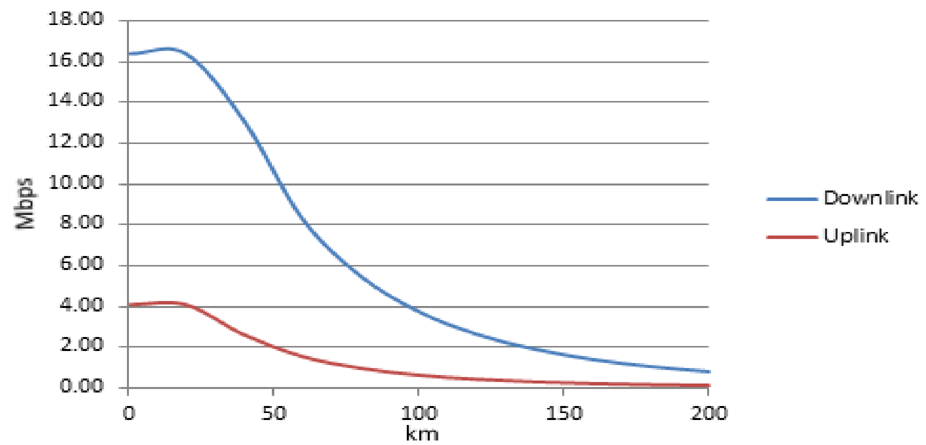


Figure 101 - Expected performance with omnidirectional antenna, for sites in close proximity to airports.

7.3.3. SoR (Statement of Requirements) Design

Although a resolution on the spectrum to be used at European level has not been achieved BT was keen to be ready in case the 5.8 GHz band becomes available. For this reason BT started creating the SoR to find the solutions proposed by vendors. The full system is divided in 6 lots of which the author was the main designer for lot 1 (avionics aboard the aircraft) and consultant for lot 2 (avionics ground to earth radio equipment) and lot 3 (UMTS TDD system) (see Figure 102). The lots would be allocated to a single lead vendor that is welcome to interact with other vendors interested to provide technology/input in the lot to deliver the complete solution.

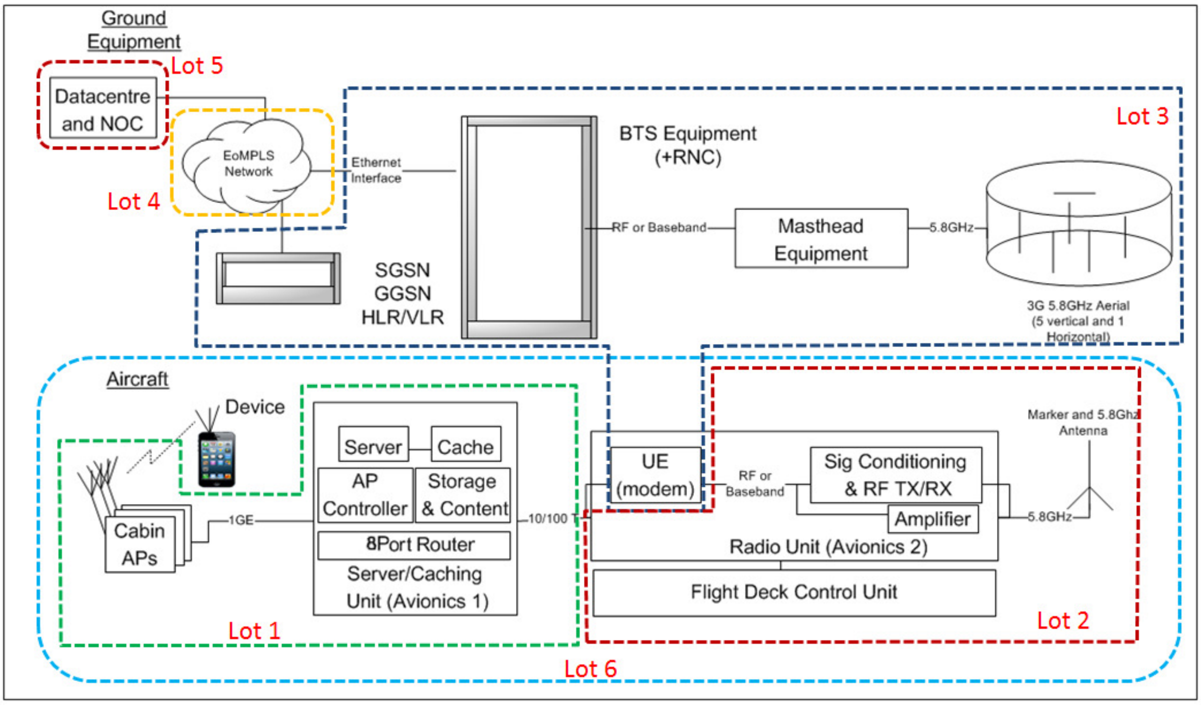


Figure 102 - Lot division of the complete solution.

For the design of the requirements in lot 1, the data from the experience gathered in the trials done with EasyJet in Section 7.3.1 was used. Therefore, the use of at least 5 non-interfering Wi-Fi APs, PoE to provide power to the APs, a cache to reduce the amount of backhaul usage, video server and DNS server were all added to the final requirement list, see Figure 103. To minimize the weight of all the equipment a requirement to virtualize all the functionality in a single server or 2 was included, and the main requirement for a vendor offering this system was to be able to provide the compulsory avionics certification for all the hardware provided.

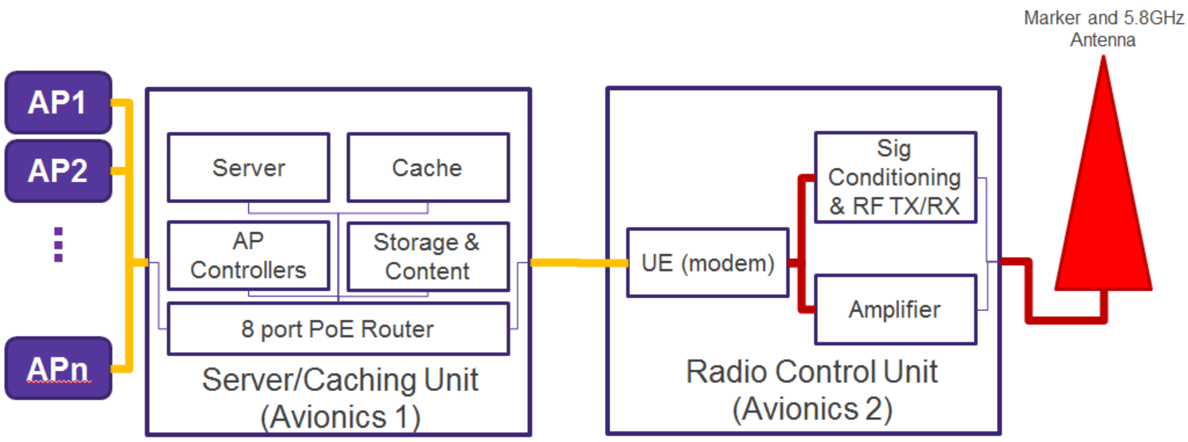


Figure 103 - Avionics units (inside equipment bay).

Chapter 8: Spectrum/Interference Management

While we move to 5G new technologies and new frequencies will become available to allow higher bandwidth in both licensed and unlicensed spectrum, but these need to be carefully chosen and used so it doesn't interfere with the existing deployed networks.

Below in Figure 104 and Figure 105, is a summary of the worldwide frequency allocation in the bands from 300 MHz to 30 GHz and an explanation of the different regions as defined by IMT.

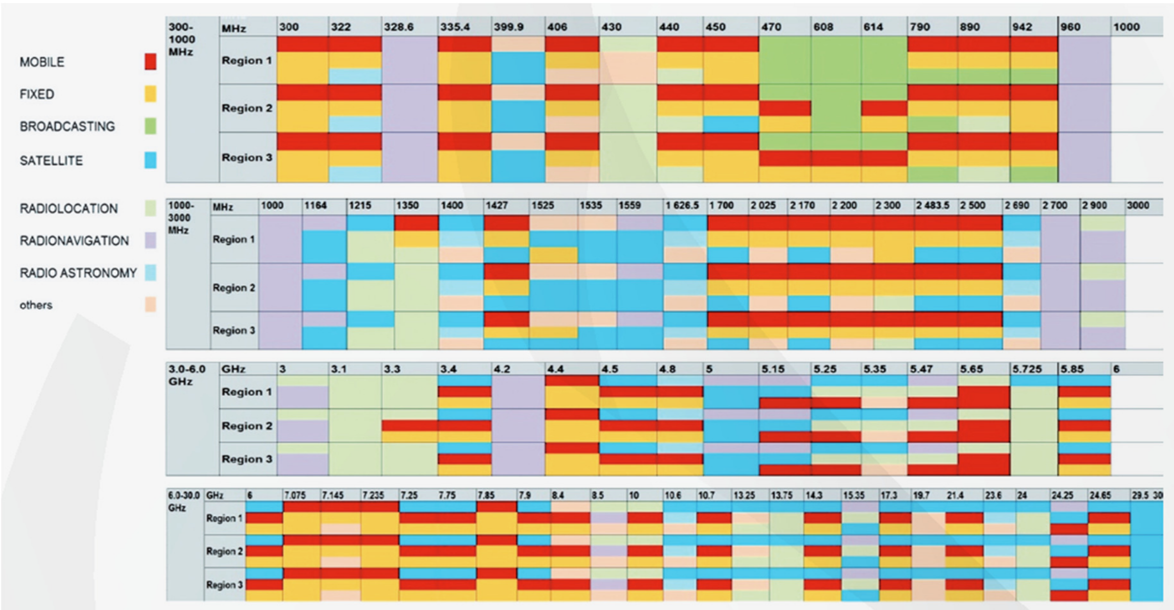


Figure 104 - Summary frequency allocation from 300 MHz to 30 GHz (Source: IMT).

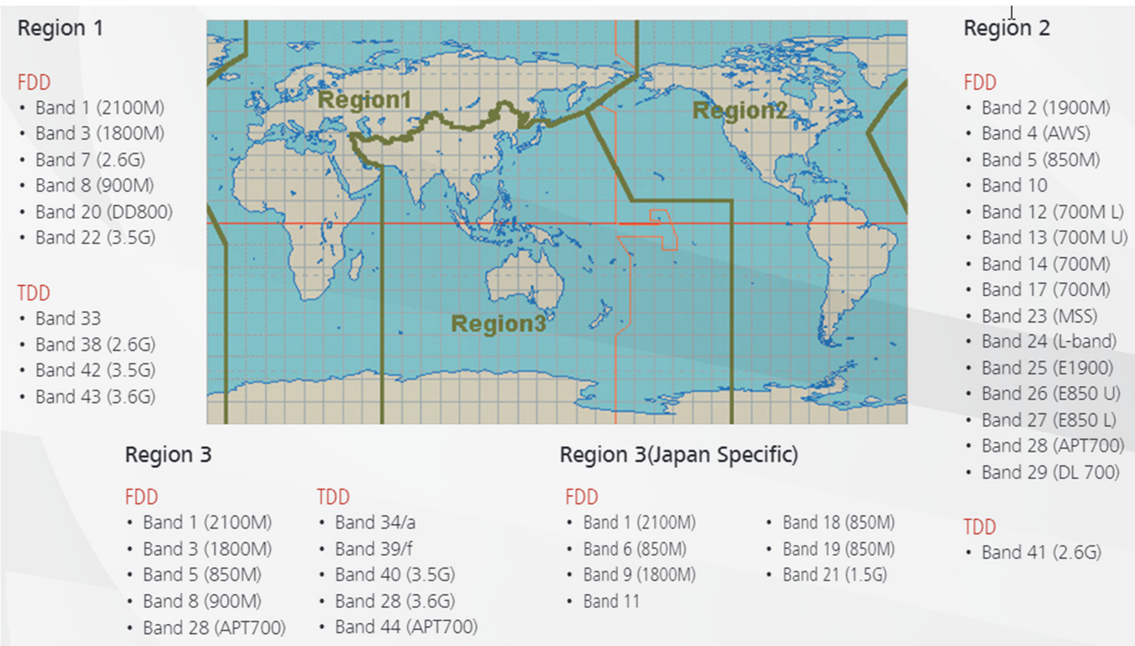


Figure 105 - IMT global spectrum distribution (existing situation) (Source: IMT).

8.1.State of the Art (2013)

Some Wi-Fi operators who have deployed 2600 MHz LTE networks are reporting that poor out-of-band rejection by some Wi-Fi devices (particularly smartphones and tablets) is leading to interference problems and reduced Wi-Fi throughput in locations where LTE networks and Wi-Fi networks are co-located [158]. In parallel, the 3GPP standards organisation has been investigating potential LTE to Wi-Fi interference for dual mode devices such as dual-mode Wi-Fi/LTE smartphones, where the Wi-Fi and LTE transceivers are in close proximity, and even where LTE uses the same unlicensed spectrum [159] [160], known as LTE-U. In Section 8.2 we perform an investigation of the interference issue within the UK assigned bands and provide recommendations. These similar concerns will arise as well when Ofcom decides to auction spectrum at 2.3 GHz (between 2350 MHz and 2390 MHz), just below the 2.4GHz Wi-Fi band [161].

In the search of extra spectrum higher frequencies are being considered like 3.5-3.6 GHz [162] and even 5 GHz [163]. Even though 3.6 GHz still allows non-line of sight communication, these frequencies are not suitable for macro coverage for a mobile service, there are usually used as indoor or small cell solutions [164] [165]. These high frequencies could potentially be used to provide a fixed wireless service with the use of external antennas. In Section 8.3 we study the performance and deployment of a 3.6 GHz LTE system to cover a rural area with slow broadband speeds and provide a broadband service comparable to broadband in urban areas. A similar system using WIMAX was deployed in Croatia to deliver a similar system [166]. In our deployment we favoured the TDD version of LTE has it allows for a better control and flexibility of upload vs download bandwidth (load balancing), doesn't need paired spectrum and it is easier to use MIMO or beamforming [167].

8.2.Wi-Fi/LTE Coexistence Tests

The interference problem is attributed to poor ACS (Adjacent Channel Selectivity) in lower cost Wi-Fi devices which causes Wi-Fi devices to perceive LTE transmissions as additional interference noise and leads to desensitisation of the Wi-Fi receiver. Receiver desensitisation leads to higher packet retry and loss rates and consequently reduced access point capacity and reduced peak user throughputs. This is a particular problem for LTE Bands 38 (2300-2400 MHz) and band 7 (2500-2600) which lie either side of the 2.4 GHz ISM Wi-Fi band. For the 2.6GHz band 7 in the UK, the main source of interference will be the uplink transmissions from mobile devices, with the Vodafone FDD uplink spectrum at 2500-2520 MHz and the BT FDD uplink spectrum at 2520-2535 MHz.

Initially, a set of laboratory based tests using a signal generator to simulate LTE devices fully loading the uplink spectrum at various transmit powers and frequencies was performed in order to study and quantify the potential interference effect of LTE devices on a Wi-Fi smartphone connected to a BT HomeHub. These tests were not extensive and were intended to determine whether further study was warranted. In these tests it was possible to cause substantial reductions (>50%) to Wi-Fi throughput at LTE power levels above 15 dBm (31 mW) and where the LTE transmitter was within 3 m of the Wi-Fi stations or access points. Impact on Wi-Fi throughput reduced as the LTE frequency increased but was still significant at a centre frequency of 2.535 GHz. When the LTE simulator was in very close proximity <1 m to the Wi-Fi device or access point then Wi-Fi data throughput could be reduced to zero across the entire 2.4 GHz band.

An attempt was also made to simulate a BT LTE femtocell scenario using a single real LTE mobile device (Huawei Ascend) connected to a Huawei enterprise picocell with uplink traffic generated using Dropbox based file uploads. In these tests there was no noticeable impact on nearby Wi-Fi throughputs. However in these tests the LTE device would be expected to use lower transmit powers and would not have fully loaded the uplink channel.

As reported by other operators, it was found that a Wi-Fi enabled laptop PC was substantially immune to LTE interference, which suggests higher quality filtering and improved out-of-band rejection in the PC Wi-Fi implementation.

Analysis of over the air Wi-Fi packet captures show that the LTE interference disproportionately affects Wi-Fi data packets which tend to be larger (>1000 bytes), make greater use of frame aggregation and are transmitted at higher data rates. Wi-Fi management packets which are smaller and tend to be sent at lower data rates were less affected resulting in the situation where the mobile device was associated to an access point at good signal strength but was unable to maintain any decent TCP throughput.

8.2.1. Summary

The tests indicate that in the worst case there is potential for LTE at 2.6 GHz to cause significant disruption to Wi-Fi services. Due to the nature of the frequency band allocation, interference would be most significant from Vodafone mobile subscribers transmitting to LTE base stations at higher powers. Problematic scenarios could for example include BT Wi-Fi public hotspot within the coverage areas of Vodafone outdoor 2.6 GHz micro cells.

The 3GPP study group results combined with BT tests with LTE transmitters in close proximity (<1 m) to Wi-Fi receivers suggest that service scenarios involving simultaneous Wi-Fi and LTE within the same device e.g. dual mode smartphone or integrated Wi-Fi/LTE access point will need careful design if Wi-Fi performance is to be maintained. Additional hardware filtering [168], more intelligent Wi-Fi channel selection or rate control algorithms may be required.

Given these initial results it is recommended that further study is undertaken with a wider range of Wi-Fi devices and access points and with non-lab based LTE usage scenarios to determine the full extent of the issue and to identify possible mitigation solutions.

8.3. Radio Performance of an LTE Network Using 3.6 GHz Spectrum

Project for Openreach in conjunction with UKB (UKBroadband) that had a license in the 3.6 GHz of up to 120 MHz of unpaired spectrum available (Figure 106, the amount of spectrum depends on the area as there are other licensees sharing it). This technology was meant to be used to cover the last 2-5% UK population that cannot receive broadband over 2-4 Mbps using LTE TDD in a similar way that was used in Section 7.[2]

This project highlights the challenges of using LTE or any other mobile/fixed wireless technology on higher frequencies over a large coverage area. Spectrum is a finite non-renewable resource and it is the basic requirement for any type of wireless communication. As more spectrum is required to be made available operators and regulators will have to try to start looking at higher bands to deploy mobile services, and although these higher bands tend to be used in small cells because of the radio properties (high propagation loss and high penetration loss), in this project it is demonstrated how it could be deployed to provide a fix wireless service from a macrocell covering an area of 7 km radius. Moreover, this project uses the TDD version of LTE which allows a more flexible utilization in fragmented spectrum as described in [169].

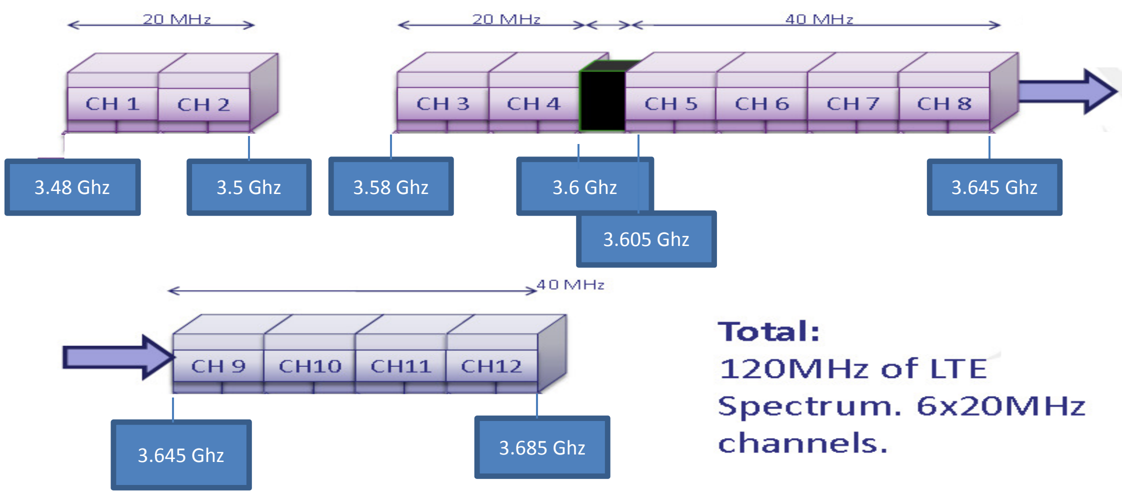


Figure 106 - UKB spectrum licenses (Source: UKB).

The assignment consists on deploying and testing the performance of a 3.6 GHz LTE TDD macrocell in Adastral Park (Ipswich). This macrocell used 3 x 20 MHz non-interfering channels (1 channel/sector) and a transmitter power of 1 kW (60 dBm). The procedure in [170] was

---

[2] Obviously after BT won spectrum licenses in the UK spectrum auction in 2.6 GHz band in 2013 this project was cancelled.

followed to decide which 20 MHz slots we would use in the selected location to avoid interfering with other licensees.

The sectors had only a 60 degree coverage (instead of 120 as usual trisector macrocells), so I had to carefully select the direction for each one to cover the maximum number of interesting points from the radio spectrum point of view.

In Figure 107, the black circle represents 7 km radius from base station:

- **Sector 1:** pointing to Little and Great Bealings and get to Hasketon and Playford (no-spot/slow areas)
- **Sector 2:** covering Sutton Waldringfield and a little of Shottisham
- **Sector 3:** covering Brightwell, Bucklesham, Nacton and Levington and some of south east Ipswich

Apart from the above Woodbridge could get some coverage from sectors 1 and 2. Similarly some coverage would fall into Kesgrave too.

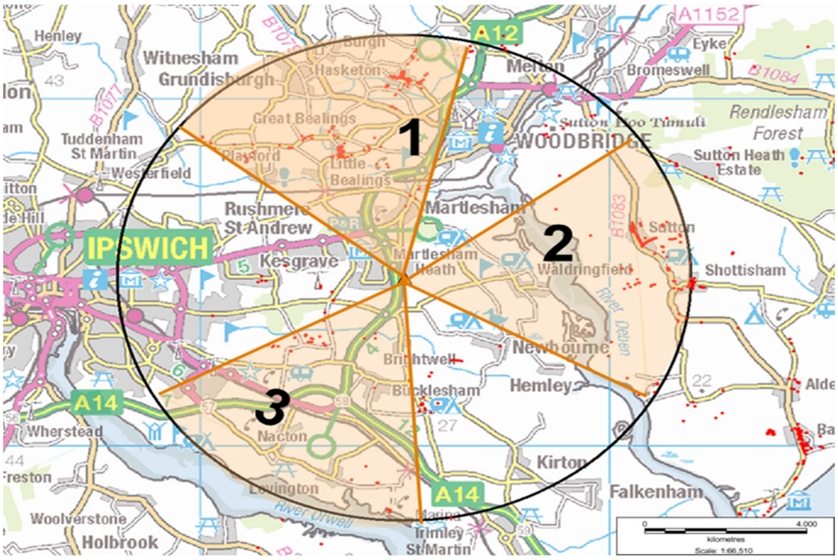


Figure 107 - 90 degrees sectors pointing towards no-spots (red dots).

The channel utilization was split 50% for uplink and 50% for downlink, this was done to improve the uplink performance as the radio conditions were more challenging for the CPE (Customer Premises Equipment) (less power, less height).

Figure 108 - Trisector 3.6GHz macrocell installed on top of Callisto House.

The mast was located on one of the roofs of Adastral Park (Callisto House), see Figure 108, at approx. 22 m (total of 47 m from sea level), although a typical installation in a rural area won't typically be able to a similar height (expected a 13 m average).

8.3.1. Methodology & Results

After the installation was completed, a coverage and performance model was created by UKB that was later compared with my data from measurements taken in over 100 locations within the coverage area, which was expected to be around 7 km. I took the measurements looking at surrounding houses at eves height (3 m) and at roof height (7-8 m).

A vehicle equipped with a pneumatic pump-up mast to lift a directional antenna (14 dBi) was used to take the measurements, see Figure 109. These measurements were taken in an uncontended network (only 1 user/sector), so it is important to take into account that speeds in a congested network will be significantly lower.

Figure 109 - Pump up mast with directional antenna.

For each location the following parameters were measured for over 2 min (see Annex B for detail):

- SINR (Signal to Interference plus Noise Ratio), RSSI (Receive Signal Strength Indication), RSRP (Reference Signal Received Power), RSRQ (Reference Signal Received Quality)
- Bars shown on CPE
- Download/Upload peak speed from FTP server on the back of EPC.
- Cell ID (sector= 91 points north west, 92 points east, 93 points south west)

I selected the following areas for testing:

- **Sutton & Shottisham**: Long range, 6 to 7 km away from the antenna, sometimes with trees covering LoS (sector 92).
- **Martlesham Heath**: very close proximity, 600 m to 1 km, half locations selected with lots of trees covering LoS, half of the locations without (sector 91/93).
- **Kesgrave**: along Playford road, mid-range (1.5-4 km) some with trees some without (sector 91).
- **Adastral Park:** across the site. Very close to eNB (within 400 m), over 25 Mbps achieved even on buildings shadow (refractions).

- **Woodbrige:** (6.8 km) no signal was received probably due to great forest mass on the radiation direction.
- **Orwell river shoreline**: Including Levington and Nacton, no signal was received probably due to degradation caused by Radio tower shadowing
- **Grundisburg, Great and Little Bealings:** within a very dense forest area (7.7 km to 3.4 km), good signal if no trees nearby due to high terrain altitude

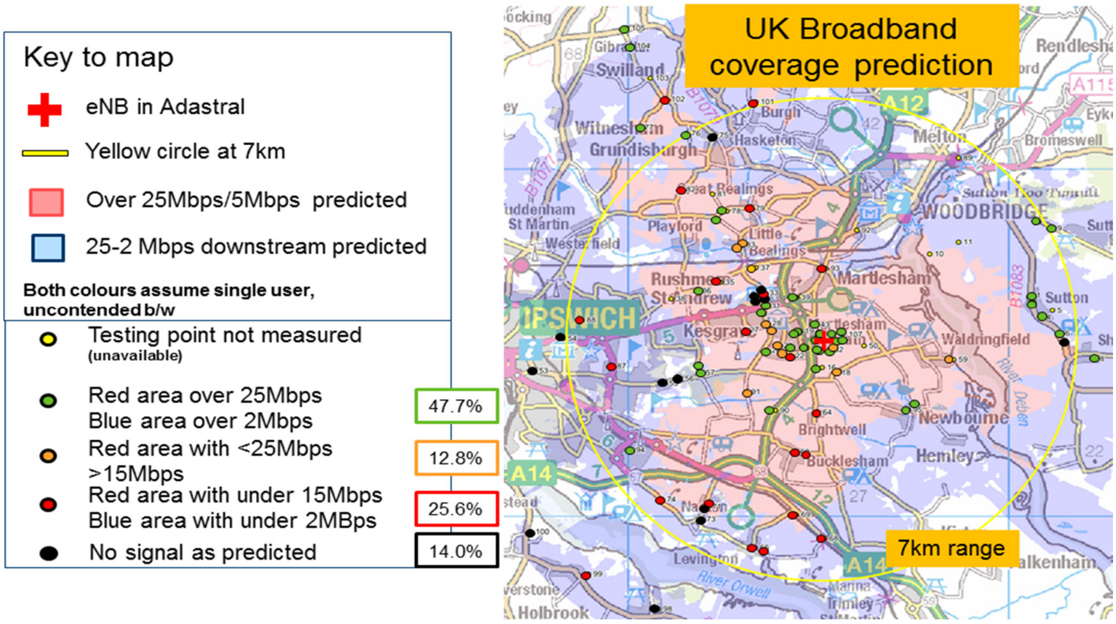


Figure 110 - UKB predicted speeds vs BT measurements. The red area is the area where speeds over 25Mbps DL and 5Mbps UL were calculated, the blue area is where between 25Mbps to 2Mbps are expected. Dots are testing locations, green means that the prediction (red/blue area) matches actual result, orange means the prediction is close to actual result, red means the prediction doesn't match actual result and black means there was no signal as predicted.

After taking these measurements, see Annex B: Measurements from 3.6GHz LTE TDD, they were compared to the UKB estimations, see Figure 110, and although there was quite a high correlation there were quite a few locations were the predicted speeds didn't correlate (25.6%) to the estimation. This was due to the lack of clutter data in the UKB predictions, which meant that to predict the performance in a real life deployment a more detailed clutter map would be required.

Effect of terrain and trees on achievable speeds

Terrain altitude has a great importance in the achieved speed, as it allows the antennas to communicate above the clutter, see Table 22.

Table 22 - Measurements at high terrain elevation and far compared to low elevation and close to macro. NOTE: All measurements done in the same angle from sector antenna.

Location	Distance	Height from sea level	Downlink 8m	Uplink 8m	Downlink 3m	Uplink 3m
Otley college	10.3 km	59 m	14.72 Mbps	2.82 Mbps	-	-
Grundisburgh	7.8 km	51 m	49 Mbps	9.84 Mbps	48 Mbps	12.8 Mbps
Little Bealings	3.5 km	13 m	16.6 Mbps	1.9 Mbps	360 kbps	60 kbps

The appearance of high trees (over 10 m) in the direction of radiation in the close proximity has a big impact in the signal received, see Table 23.

Table 23 - Comparison between locations with and without surrounding trees

Location	Distance	Height from sea level	Downlink 8m	Uplink 8m	Downlink 3m	Uplink 3m
Great Bealings (surrounded by high trees)	4.3 km	21 m	-	-	-	-
Great Bealings	4.4 km	19 m	43 Mbps	11.3 Mbps	30 Mbps	5 Mbps

An immediate amount of dense forest area can also lower the performance of the system, see Table 24. This result was already expected from looking at results of similar systems like [171] where it is demonstrated that the amount of foliage (which changes depending on the season) has a dramatic effect on the system performance. The only way to avoid it is to use the highest point in the house for the antenna placement.

Table 24 - Comparison with and without dense forest area in the direction of propagation.

Location	Distance	Height from sea level	Downlink 8m	Uplink 8m	Downlink 3m	Uplink 3m
Martlesham Heath (in front of forest area)	0.7 km	24 m	48 Mbps	14.72 Mbps	49 Mbps	12.9 Mbps
Martlesham Heath (same angle behind forest)	0.95 km	28 m	15 Mbps	1.83 Mbps	11.2 Mbps	1.2 Mbps

Buildings greatly reduce achievable bitrates

In sector 93 (facing south west from Adastral) the results are much worse than in the other 2 sectors. The reason for this is that sector 93 radio waves had to clear the radio tower in

Adastral Park, which is a big obstacle (200 feet tall) and it creates a radio shadow (area without coverage). For example, in Figure 111 in Bucklesham (point 1) at 3.2 km with clear view of the tower no signal is received at 8 m or 3 m. A few meters away from this location (point 2) at the same distance from the eNB and with some local clutter 3.66 Mbps/1.68 Mbps are achieved, suggesting that we are moving away from the shadowed area.

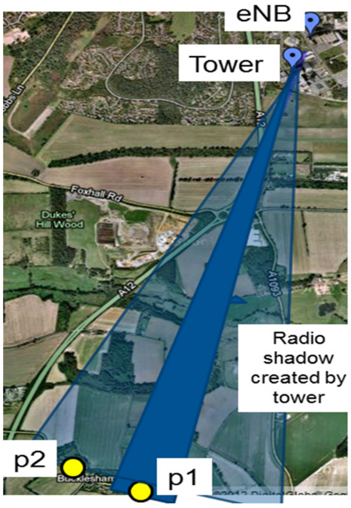


Figure 111 - Shadowed area from South west facing sector.

UL/DL Speed vs RSSI correlation

UL/DL Speed is highly correlated to the RSSI indicator (in uncontended conditions), see Figure 112. This was expected has the better RSSI, the higher modulation scheme can be used in the transmission and therefore higher speeds are achievable.

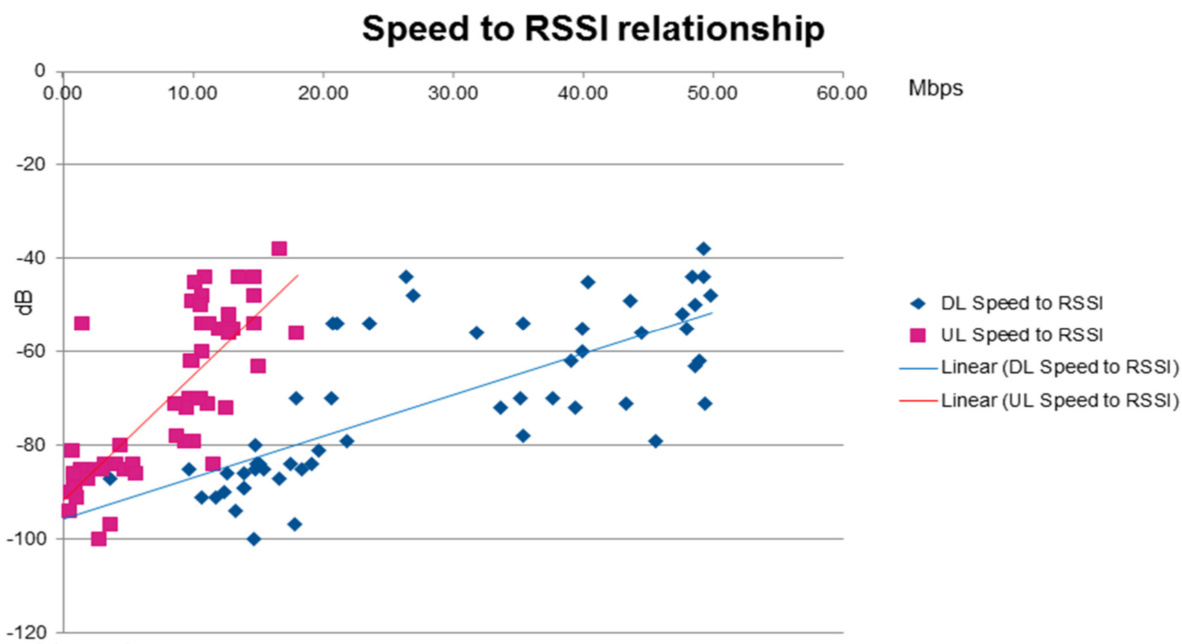


Figure 112 - UL and DL speed correlation to RSSI.

8.3.2. Summary

The service can deliver high headline rates in good coverage – up to 50 Mbps down, 15 Mbps up with current CPE close to the base station and 15 Mbps down, 3 Mbps at 10 km were seen. Sufficient height for end-user CPE is critical to gaining service in marginal coverage. Moving from eves height to rooftop would make a useful difference.

The technology and equipment is essentially the same as mobile operators deploy for LTE, just operating at 3.5 GHz implying a similar cost base, but without the ability to leverage existing assets (base station infrastructure, customer base etc.) and with poorer coverage.

From the measurements taken we found that the UKB predictions had been slightly optimistic with a 74.5% accuracy (green, yellow and black dots), after questioning UKB on their process we discovered they didn't had accurate enough clutter data for the area which explains some of the distortion. With the appropriate clutter data predictions can be made before installation, which can be used for radio access network design and planning.

Chapter 9: Conclusions and Future Work

The past and current status of the wireless heterogeneous environment has been analysed in this thesis. This has highlighted some of the current heterogeneous environment deficiencies. Based on the problems found it has presented a few solutions and developments for some problematic areas to help move current wireless networks towards the 5G requirements.

Firstly, one of the earliest 802.21 based MIIS using early drafts and the final standard was implemented, and feedback was given for improvements via the interoperability event in FMCA headquarters in Sophia Antipolis (October 2009). During this IOT event the MIH proxy was also tested with other vendors developed MIH Servers allowing for a better integration of different vendor solutions, and hence, making it possible to leave the standard open with several options for implementation, as the MIH proxy would re-direct or translate between the different information presentation options chosen by different vendors. Because of the zero-touch unobtrusive user experience provided, MIH or similar technologies that enable seamless handover and session continuity in a heterogeneous wireless environment need to form part of the strategy that would transform the current networks into 5G networks.

Secondly, to maintain the seamlessness and unobtrusivity of the user experience provided by MIH it is needed one single method for seamless authentication with all the involved wireless networks. 802.1x using the SIM credentials (the same that are used in the mobile networks) with EAP-SIM/AKA/AKA' is ideally placed to perform the task, as it means the authentication converges in one single point on the mobile network architecture, the HSS/HLR/AuC. This of course, will not be possible in already deployed Wi-Fi networks without major re-designs, for this reason a solution that could overcome the problem of zero-touch seamless authentication for Wi-Fi networks without a big investment was investigated. This solution, in Section 5.3, was filed as a patent in 2010, and tries to reuse the knowledge of the available access points in a location that a server like the 802.21 MIIS would have, the overlap of coverage between Wi-Fi networks and mobile networks to detect, select and authenticate the target Wi-Fi network using the already secure establish mobile connection.

While studying big Wi-Fi deployments, it was noticed the fact that a lot of these access points or mobile small cells would be self-installed. This would mean that unless the connection between the small cell and the core of the mobile network was secured with IPSec or similar, the connection would be insecure. Therefore, this implies an increase of secure tunnels over 100 times the current secured connections to base stations the mobile networks support. In Section 5.4, in collaboration with Stoke Inc., the performance of a SeGW that would handle the secure connectivity with the core network was tested, diminishing the impact of the 100x increase in base stations. During the performance of this test, the possible implications in case the mobile operators wanted to deliver content closer to the edge of the network were noticed, which wouldn't be possible if the connection is secured E2E unless the SeGW is also transported to the edge.

The performance of an edge content delivery solution by Saguna was studied and tested, and a new content delivery technique for mobile networks was developed, which was filed as a patent in 2013. This solution tries to find the more efficient way to deliver content to each user, depending on: the user location, the content location, the cost associated to each path the content could take and current usage and congestion in the network. An implementation of this solution has not been possible yet, but it could be an interesting point for further study.

After looking at the 3 areas above a few techniques or tools had already been found that could potentially help in delivering the results that had been set as a target, but these results could not be achieved in all locations, and therefore would not completely fulfil the ideal connectivity environment. Places like rural locations or public transport would still lag behind the connectivity received by larger urban environments with easier to reach radio conditions. Participating in the first LTE MOCN network (between EE and BT), a series of experiments to increase the user experience of the BT subscribers while avoiding affecting the service of the EE trialist were allowed. The feedback received provided great insights on how a shared RAN in a rural area could be managed and tweaked to independently address both mobile and fixed users from two different operators.

Following the investigation on rural infill, looking into high density modes of transport, the opportunity to work on the BT Danube project appeared, which aimed to use a modified UMTS TDD system to deliver connectivity to planes across Europe. The plane to ground path loss was calculated and an estimation of the expected bandwidth, which correlated closely to the live test data supplied by Aero3G, was delivered as an output. Consequently, the effort was put in how to improve the user experience within the plane with the available backhaul, using 2.4 GHz and 5 GHz Wi-Fi, band steering, high density Wi-Fi techniques and content caching, and proved their success in a live trial inside an actual plane borrowed from EasyJet. The knowledge gained in this trial was used in the Statements of Requirements that were written subsequently for vendors to bid in.

Finally, a study of the impact of the interference of the new LTE bands auctioned by the UK government was carried on. This study demonstrated that the uplink of the band closer to Wi-Fi 2.4 GHz could definitely interfere in the scenarios where a device was trying to reach a faraway macro antenna (higher signal strength used) and where cheaper Wi-Fi chipsets without adequate filtering are used. These results were fed back into the 3GPP study group looking at the issue. At the same time, it is clear that new spectrum at higher bands is required for mobile networks to increase the bandwidth in their deployments, therefore a test in a macrocell radiating at 3.6 GHz to assess its performance was carried out, this showed that although possible this kind of spectrum is really more suited for small cell scenarios.

From the different projects involved during the length of this thesis, it is expected that in the future innovative solutions similar or based in the tools provided will be used to resolve some of the main requirements to evolve the current networks into 5G. Achieving high data rates in standard main stream scenarios is not as complicated as achieving a consistent user experience no matter what environment. To succeed in this last point, all available radio resources need to be seamlessly integrated and secured avoiding interference, content need to be properly and efficiently distributed to avoid unnecessary delays and costs, and the challenging radio environments need to be addressed to avoid having a big unbalance on user experience.

Future directions of research could involve:

- The management of the radio interfaces of a device to follow the mobile operator wireless strategy regarding Wi-Fi and small cells. Using the technologies in Chapter 4 the handover between heterogeneous technologies would be seamless and therefore if the MNO had the ability to control the radio interfaces an improvement in the user experience is expected.
- Securely and selectively offload data as close to the edge of the network as possible to improve latency and lower costs, as described in Chapter 5 and 6. As seen in Section 5.4, secure tunnels need to be adapted to the architecture and needs of each MNO. Core network element virtualization and edge content delivery would be key to further lower the latency.
- Research on innovative solutions to share spectrum, like Chapter 7.2, equipment or both in rural areas to improve user experience and the economics to deliver a similar service to the one offered in urban areas.
- Research improved backhaul methods to deliver higher bandwidth connectivity to airplanes, as seen in Section 7.3, the bandwidth of all SoA is limited and not comparable to the bandwidth available on land.

References

[1] FMCA, "FMCA Priority Programme #02: Converged Devices & Access Points," 24 April 2008. [Online]. Available: http://www.ieee802.org/21/email21/doc00086.doc. [Accessed 2011 August 2013].

[2] Software Informer, "iSIP," BT plc, 21 September 2009. [Online]. Available: http://isip.software.informer.com/3.0/.

[3] F. M. Abinader, E. P. L. Almeida, F. S. Chaves, A. M. Cavalcante, R. D. Vieira, R. C. D. Paiva, A. M. Sobrinho, S. Choudhury, E. Tuomaala, K. Doppler and V. A. Sousa, "Enabling the coexistence of LTE and Wi-Fi in unlicensed bands," *IEEE Communications Magazine ,* vol. 52, no. 11, pp. 54-61, 2014.

[4] M. Matinmikko, M. Palola, H. Saarnisaari, M. Heikkilä, J. Prokkola, T. Kippola, T. Hänninen, M. Jokinen and S. Yrjölä, "Cognitive Radio Trial Environment: First Live Authorized Shared Access-Based Spectrum-Sharing Demonstration," *IEEE Vehicular Technology Magazine,* vol. 8, no. 3, pp. 30-37, 2013.

[5] T. Nihtilä, V. Tykhomyrov, O. Alanen, M. Uusitalo, A. Sorri, M. Moisio, S. Iraji, R. Ratasuk and N. Mangalvedhe, "System performance of LTE and IEEE 802.11 coexisting on a shared frequency band," in *Wireless Communications and Networking Conference (WCNC)*, Shangai, 2013.

[6] Simplify Digital, "EE Launches 4g LTE home broadband in rural cumbria," Simplify Digital, 11 November 2013. [Online]. Available: http://www.simplifydigital.co.uk/news/articles/2013/11/ee-launches-4g-lte-home-broadband-in-rural-cumbria/. [Accessed 8 April 2014].

[7] X. Jover Segura and F. el-Moussa, "Method and system for authenticating a point of access". US Patent US20130019298/EP2372971A1/ EP2553898A1/WO2011121294A1, 17 January 2013.

[8] X. Jover Segura and M. Cuevas, "Gateway Reselection". Worldwide Patent PCT/GB2013/000137, 27 March 2013.

[9] X. Jover Segura, "QoE in Femtocells," in *London Communications Symposium*, London, 2010.

[10] Ofcom, "Call for Input: Measuring mobile quality of experience," 01 2013. [Online]. Available: http://stakeholders.ofcom.org.uk/binaries/consultations/mobile-voice-data-experience/summary/condoc.pdf. [Accessed 1 08 2014].

[11] K. De Moor, I. Ketyko, W. Joseph, T. Deryckere, L. De Marez, L. Martens and G. Verleye, "Proposed Framework for Evaluating Quality of Experience in a Mobile, Testbed-oriented Living Lab Setting," *Mobile Networks and Applications,* pp. 378-391, June 2010.

[12] O. Oyman and S. Singh, "Quality of experience for HTTP adaptive streaming services," *IEEE Communications Magazine,* vol. 50, no. 4, pp. 20-27, 2012.

[13] K. Zheng, X. Zhang, Q. Zheng, W. Xiang and L. Hanzo, "Quality-of-experience assessment and its application to video services in lte networks," *IEEE Wireless Communications ,* vol. 22, no. 1, pp. 70 - 78, 2015.

[14] M. Fiedler, T. THossfeld and P. Tran-Gia, "A generic quantitative relationship between quality of experience and quality of service," *IEEE Network ,* vol. 24, no. 2, pp. 36 - 41, 2010.

[15] G. Klemens, The Cellphone: The History and Technology of the Gadget That Changed the World, ebook: McFarland, 2010.

[16] B. Crow, M. Longford and K. Sawchuk, The Wireless Spectrum: The Politics, Practices, and Poetics of Mobile Media, Toronto: University of Toronto Press, 2010.

[17] D. Wisely, P. Eardley and L. Burness, IP for 3G: networking technologies for mobile communications, London: John Wiley & Sons, 2002.

[18] B. Kim, The Library Mobile Experience: Practices and User Expectations, ebook: American Library Association, 2013.

[19] A. Kivi, Mobile Internet usage measurements : case Finland, Helsinki: Department of Industrial Engineering and Management, Helsinki University of Technology, 2006.

[20] Agilent Technologies, "France Telecom Go For WiFi Wireless - Press Release," 7 February 2003. [Online]. Available: http://www.3g.co.uk/PR/Feb2003/4849.htm. [Accessed 22 September 2014].

[21] T-Mobile USA, "T-Mobile Launches Handspring Treo 270," 3 March 2003. [Online]. Available: http://www.t-

mobile.com/company/PressReleases_Article.aspx?assetName=Prs_Prs_20030304. [Accessed 20 September 2014].

[22] GSMA - Deloitte, “What is the impact of mobile telephony on economic growth,” GSMA, London, 2012.

[23] C. Coursaris, K. Hassanein, M. Head and N. Bontis, “The impact of distractions on the usability and the adoption of mobile devices for wireless data services,” in *European Conference on Information Systems*, Geneva, 2007.

[24] Chetan Sharma Consulting, “Global Wireless Data Market Update 2007,” Chetan Sharma Consulting, 2008.

[25] M. Mace, “The shape of the smartphone and mobile data markets,” January 2007. [Online]. Available: http://mobileopportunity.blogspot.co.uk/2007/01/shape-of-smartphone-and-mobile-data.html. [Accessed 22 September 2014].

[26] R. Entner, “The Data Tsunami Is Gathering Strength,” Recon Analytics, 14 June 2011. [Online]. Available: http://reconanalytics.com/2011/06/the-data-tsunami-is-gathering-strength/. [Accessed 15 September 2014].

[27] Analysys Mason, “Mobile data will grow 6.3 times between 2013 and 2018 and growth will be strongest outside Europe and North America,” Oct 2013. [Online]. Available: http://www.analysysmason.com/About-Us/News/Insight/Mobile-data-Oct2013/.

[28] M. Kurk, “Indoor Wireless Coverage: the Challenges,” radio-electronics.com, 17 June 2014. [Online]. Available: http://www.radio-electronics.com/articles/antennas-propagation/indoor-wireless-coverage-the-challenges-115.

[29] C. Rick, “4K Streaming Video - The Future Bandwidth Monster?,” Reelseo, 18 December 2013. [Online]. Available: http://www.reelseo.com/4k/. [Accessed 7 November 2014].

[30] A. de la Oliva, C. Bernardos, M. Calderon, T. Melia and J. Zuniga, “IP flow mobility: smart traffic offload for future wireless networks,” *Communications Magazine, IEEE*, vol. 49, no. 10, pp. 124 - 132, 2011.

[31] D. Cory von Wallenstein, “User experience is the new differentiator. How will that affect the internet?,” Gigaom, 20 April 2014. [Online]. Available:

https://gigaom.com/2014/04/20/user-experience-is-the-new-differentiator-how-will-that-affect-the-internet/. [Accessed 19 August 2014].

[32] B. Giles, "iOS Carrier Bundles Demystified," 4 October 2012. [Online]. Available: https://beaugil.es/2012/10/ios-carrier-bundles-demystified/. [Accessed 16 August 2014].

[33] L. Frenzel, "The Evolution Of LTE," Electronic Design, 8 January 2013. [Online]. Available: http://electronicdesign.com/content/evolution-lte. [Accessed 20 August 2014].

[34] S. Akhtar, "2G-5G Networks: Evolution of Technologies, Standards, and Deployment," 2008. [Online]. Available: http://www.irma-international.org/viewtitle/17444/. [Accessed 22 September 2014].

[35] 3GPP, "GPRS & EDGE," 3GPP, [Online]. Available: http://www.3gpp.org/technologies/keywords-acronyms/102-gprs-edge . [Accessed 21 September 2014].

[36] I. Poole, "GSM EDGE Tutorial," radio-electronics.com, [Online]. Available: http://www.radio-electronics.com/info/cellulartelecomms/gsm-edge/basics-tutorial-technology.php. [Accessed 15 September 2014].

[37] A. Usman, "Gsm (Part 1)," 6 January 2013. [Online]. Available: http://www.slideshare.net/AliUsman10/gsm-part-1. [Accessed 3 December 2014].

[38] Computer Weekly, "2G mobile services grow rapidly," Computer Weekly, May 2004. [Online]. Available: http://www.computerweekly.com/feature/2G-mobile-services-grow-rapidly. [Accessed 23 September 2014].

[39] M. C. Chuah and Q. Zhang, "End-to-End performance in 3G Networks," in *Design and Performance of 3G Wireless Networks and Wireless LANs*, New York, Springer Science & Business Media, 2005, pp. 225-228.

[40] I. Poole, "HSPA - High Speed Packet Access Tutorial," Radio-Electronics.com, [Online]. Available: http://www.radio-electronics.com/info/cellulartelecomms/3g-hspa/umts-high-speed-packet-access-tutorial.php. [Accessed 25 September 2014].

[41] I. Maradi, "Do we need Next GenerationMobile Networks ? Yes.," 2008. [Online]. Available:

http://www.networks2008.hu/data/upload/file/Plenary/P3_2_Maradi.pdf. [Accessed July 2010].

[42] I. Poole, “3G LTE Long Term Evolution Tutorial & Basics,” Radio-electronics.com, [Online]. Available: http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/3g-lte-basics.php. [Accessed 25 September 2014].

[43] LSTI Forum, “Latest results from the LTE/SAE Trial Initiative,” February 2009. [Online]. Available: http://www.lstiforum.org/file/news/Latest_LSTI_Results_Feb09_v1.pdf. [Accessed August 2013].

[44] T. Taleb, K. Samdanis and A. Ksentini, “Supporting Highly Mobile Users in Cost-Effective Decentralized Mobile Operator Networks,” *Vehicular Technology, IEEE Tr ,* vol. 63, no. 7, pp. 3381 - 3396, 2014.

[45] K. Werner, H. Asplund, D. Figueiredo, N. Jalden and B. Halvarsson, “LTE-advanced 8×8 MIMO measurements in an indoor scenario,” in *International Symposium on Antennas and Propagation (ISAP)*, Nagoys, 2012.

[46] ETSI, “ETSI Summit on Future Mobile and Standards for 5G,” 25 November 2013. [Online]. Available: http://www.3gpp.org/news-events/conferences/1515-etsi-summit-on-future-mobile-and. [Accessed 15 August 2014].

[47] L. E. Frenzel, “Ultra Wideband: Get Ready For The Next Wireless Wave,” Electronic Design, 15 October 2001. [Online]. Available: http://electronicdesign.com/communications/ultra-wideband-get-ready-next-wireless-wave. [Accessed 13 August 2014].

[48] A. Bleicher, “Millimeter Waves MayBe the Future of 5G Phones,” IEEE Spectrum, August 2013. [Online]. Available: http://spectrum.ieee.org/telecom/wireless/millimeter-waves-may-be-the-future-of-5g-phones. [Accessed August 2014].

[49] H. Elgala, R. Mesleh and H. Haas, “Indoor optical wireless communication: potential and state-of-the-art,” *IEEE Communications Magazine ,* vol. 49, no. 9, pp. 56-62, 2011.

[50] S. F. Yunas, M. Valkama and J. Niemelä, “Spectral efficiency of dynamic DAS with extreme down-tilt antenna configuration,” in *2014 IEEE 25th Annual International*

Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC), Washington DC, 2014.

[51] F. Fitzek and M. Katz, "Cognitive Wireless Networks: Concepts, Methodologies and Visions Inspiring the Age of Enlightenment of Wireless Communications," Springer Science & Business Media, 2007, p. 556.

[52] I. Poole, "IEEE 802.11b," Radio-electronics.com, [Online]. Available: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11b.php. [Accessed 25 September 2014].

[53] I. Poole, "IEEE 802.11a," Radio-electronics.com, [Online]. Available: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11a.php. [Accessed 25 September 2014].

[54] I. Poole, "IEEE 802.11g Wi-Fi Tutorial," Radio-electronics.com, [Online]. Available: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11g.php. [Accessed 25 September 2014].

[55] I. Poole, "IEEE 802.11n Standard," Radio-electronics.com, [Online]. Available: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11n.php. [Accessed 25 September 2014].

[56] BT plc, "BT Wi-fi launches new Windows Phone app as hotspot numbers pass 7.5 million," BT plc, December 2012. [Online]. Available: http://www.btplc.com/News/Articles/Showarticle.cfm?ArticleID=1DA0EC54-0568-4FBE-A5D5-D8C111876678. [Accessed 26 September 2014].

[57] Coleago Consulting, "Whitepaper: Will Wi-Fi relieve congestion on cellular networks," 5 May 2014. [Online]. Available: http://www.gsma.com/spectrum/wp-content/uploads/2014/05/Wi-Fi-Offload-Paper.pdf. [Accessed 26 September 2014].

[58] 3GPP, "3GPP TR 23.852 - Study on S2a Mobility based on GPRS Tunnelling Protocol (GTP) and Wireless Local Area Network (WLAN) access to the Enhanced Packet Core (EPC) network (SaMOG); Stage 2," 27 April 2011. [Online]. Available: http://www.3gpp.org/DynaReport/23852.htm. [Accessed 15 August 2014].

[59] S. Hansell, "Steve Jobs's Home Run With the iPhone," The New York Times, 22 October 2008. [Online]. Available:

http://bits.blogs.nytimes.com/2008/10/22/steve-jobss-home-run-with-the-iphone/?_r=0. [Accessed 26 September 2014].

[60] BT plc, “Harnessing the data tsunami,” BT plc, Ipswich, 2012.

[61] E. Phneah, “Operators need to stick together to fend off OTT players,” ZDNet, 5 June 2012. [Online]. Available: http://www.zdnet.com/article/operators-need-to-stick-together-to-fend-off-ott-players/. [Accessed 26 September 2014].

[62] MobileAware, “Reclaiming a Lost Opportunity: Why Mobile Network Operators Missed Out on the App Economy,” April 2013. [Online]. Available: http://www.mobileaware.com/wp-content/uploads/2013/04/MNO-Gateway-App-Strategy.pdf.

[63] H. Choi, “CJK white paper on Forecast of mobile broadband development in the Asia-Pacific Region.,” September 2011. [Online]. Available: http://www.tta.or.kr/English/new/external_relations/meetingDocumentView.jsp?boardIdx=IMT&num=109.

[64] A. Iera, C. Floerkemeier, J. Mitsugi and G. Morabito, “The Internet of things,” *IEEE Wireless Communications,* vol. 17, no. 6, pp. 8-9, 2010.

[65] T. Pötsch, S. N. K. K. Marwat, Y. Zaki and C. Gorg, “Influence of future M2M communication on the LTE system,” in *Wireless and Mobile Networking Conference* , Dubai, 2013.

[66] S. Počuča and D. Giljević, “Machine to machine (M2M) communication impacts on mobile network capacity and behaviour,” in *MIPRO*, Opatija, 2012.

[67] Cisco, “Architecture for Mobile Data Offload over Wi-Fi Access Networks,” Cisco, 2012. [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-wi-fi/white_paper_c11-701018.html. [Accessed October 2014].

[68] K. Lee, J. Lee, Y. Yi, I. Rhee and S. Chong, “Mobile data offloading: how much can WiFi deliver?,” in *Co-NEXT '10*, New York, 2010.

[69] S. Dimatteo, P. Hui, B. Han and V. O. K. Li, “Cellular Traffic Offloading through WiFi Networks,” in *IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS)*, Valencia, 2011.

[70] D. H. Hagos, The Performance of WiFi Offload in LTE, Luleå: Luleå University of Technology, 2012.

[71] M. Shi, X. Shen and J. W. Mark, "IEEE 802.11 roaming and authentication in wireless LAN/cellular mobile networks," *IEEE Wireless Communications,* vol. 11, no. 4, pp. 66-75, 2004.

[72] M. Navali, K. Chowdhury, S. K. Puthiyandyil and M. Harper, "Internet protocol tunneling on a mobile network". US,WO Patent US 20070189219 A1, 16 August 2007.

[73] I. Szekely, T. Balan, F. Sandu, D. Robu and S. Cserey, "Optimization of GSM-UMTS core network for IP convergence in 4G through Mobile IPv6," in *11th International Conference on Optimization of Electrical and Electronic Equipment*, Brasov, 2008.

[74] S. Singh, H. Dhillon and J. Andrews, "Offloading in Heterogeneous Networks: Modeling, Analysis, and Design Insights," *Wireless Communications, IEEE,* vol. 12, no. 5, pp. 2484 - 2497 , 2013.

[75] V. G. Gupta and P. Jain, "Trusted wlan connectivity to 3gpp evolved packet core". US,CN and 55 more Patent US 20140101726 A1, 10 April 2014.

[76] R. Copeland and N. Crespi, "Policies to Enable Serving Untrusted Services on Alternative (Non-3GPP) and Untrusted Access Networks in EPS," in *IEEE 35th Annual Computer Software and Applications Conference Workshops (COMPSACW)*, Munich, 2011.

[77] Ruckus Wireless, Inc. , "White paper: Integrating Wi-Fi RANs into theMobile Packet Core," April 2014. [Online]. Available: http://a030f85c1e25003d7609-b98377aee968aad08453374eb1df3398.r40.cf2.rackcdn.com/wp/wp-integrating-wifi-rans-into-the-mobile-packet-core.pdf. [Accessed May 2014].

[78] R. Valmikam and R. Koodli, " DRAFT: EAP Attributes for Wi-Fi - EPC Integration," 14 November 2014. [Online]. Available: https://tools.ietf.org/html/draft-ietf-netext-wifi-epc-eap-attributes-14. [Accessed 28 11 2014].

[79] D. Chambers, "Femto Forum expands to become the Small Cell Forum," ThinkSmallCell.com, 15 February 2012. [Online]. Available: http://www.thinksmallcell.com/Latest/femto-forum-expands-to-become-the-small-cell-forum.html. [Accessed 22 September 2013].

[80] S. Chen, Y. Wang, F. Qin, Z. Shen and S. Sun, "LTE-HI: A new solution to future wireless mobile broadband challenges and requirements," *Wireless Communications, IEEE,* vol. 21, no. 3, pp. 70 - 78, 2014.

[81] WifiNigel, "Wifi channels on 5 GHz in UK," 23 September 2012. [Online]. Available: http://wifinigel.blogspot.co.uk/2012/09/wifi-channels-on-5ghz-in-uk.html. [Accessed 25 September 2014].

[82] IEEE, "IEEE 802.11s: The WLAN Mesh Standard," *IEEE Wireless Communications,* vol. 17, no. 1, pp. 104-111, 2010.

[83] N. Balasubramanian, A. Balasubramanian and A. Venkataramani, "Energy consumption in mobile phones: a measurement study and implications for network applications," in *Internet Measurement Conference*, New York, 2009.

[84] N. Ding, D. Wagner, X. Chen, A. Pathak, Y. C. Hu and A. Rice, "Characterizing and modeling the impact of wireless signal strength on smartphone battery drain," in *nternational conference on Measurement and modeling of computer systems SIGMETRICS*, New York, 2013.

[85] V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert, "Nemo Basic Support Protocol," IETF, 2003.

[86] E. N. Leymann, C. Heidemann and X. Li, "GRE Notifications," IETF, 2013.

[87] F. Liu, E. Erkip, M. Beluri, R. Yang and E. Bala, "Dual-band femtocell traffic balancing over licensed and unlicensed bands," in *IEEE International Conference on Communications (ICC)*, Ottawa, 2012.

[88] K. Taniuchi, Y. Ohba, V. Fajardo, S. Das, M. Tauil, Y.-H. Cheng, A. Dutta, D. Baker, M. Yajnik and D. Famolari, "IEEE 802.21: Media independent handover: Features, applicability, and realization," *Communications Magazine, IEEE,* vol. 47, no. 1, pp. 112 - 120 , 2009.

[89] H. Liu, C. Maciocco, V. Kesavan and A. L. Y. Low, "Energy efficient network selection and seamless handovers in Mixed Networks," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops*, Kos, 2009.

[90] P. Neves, F. Fontes, S. Sargento, M. Melo and K. Pentikousis, “Enhanced Media Independent Handover Framework,” in *Vehicular Technology Conference*, Barcelona, 2009.

[91] J. Yuan, Y. Wang, F. Liu and L. Zheng, “Optimized Handover Scheme Using IEEE 802.21 MIH Service in Multi-Service Environment,” in *Vehicular Technology Conference* , Taipei, 2010.

[92] G. Lampropoulos, C. Skianis and P. Neves, “Optimized fusion of heterogeneous wireless networks based on media-independent handover operations,” *Wireless Communications, IEEE,* vol. 17, no. 4, pp. 78 - 87, 2010.

[93] R. Tamijetchelvy and G. Sivaradje, “An optimized fast vertical handover strategy for heterogeneous wireless access networks based on IEEE 802.21 media independent handover standard,” in *Advanced Computing (ICoAC)*, Chenai, 2012.

[94] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong and J. C. Zhang, “What Will 5G Be?,” *IEEE Journal on Selected Areas in Communications ,* vol. 32, no. 6, pp. 1065 - 1082, 2014.

[95] S.-L. Huang, “Evolution from 3G to 4G and beyond (5G),” in *ITN-620 Enterprise Network Design* , 2005.

[96] A. Scrase, “ETSI Summit on Future Mobile and Standards for 5G Conclusions,” 25 November 2013. [Online]. Available: http://docbox.etsi.org/Workshop/2013/201311_FUTUREMOBILESUMMIT/ZZ_CONCLUSIONS.pdf. [Accessed 15 August 2014].

[97] 3GPP, “ETSI Summit on Future Mobile and Standards for 5G,” 3GPP, 25 November 2013. [Online]. Available: http://www.3gpp.org/news-events/conferences/1515-etsi-summit-on-future-mobile-and.

[98] U. Varshney and R. Jain, “Issues in emerging 4G wireless networks,” *Computer ,* vol. 34, no. 6, pp. 94 - 96, 2001.

[99] A. Arjona and H. Verkasalo, “Unlicensed Mobile Access (UMA) Handover and Packet Data Performance Analysis,” in *ICDT '07. Second International Conference on Digital Telecommunications*, San Jose, CA, 2007.

[100] N. Seta, H. Miyajima, L. Zhang, H. Hayashi and T. Fujii, "All-SIP Mobility: Session Continuity on Handover in Heterogeneous Access Environment," in *VTC2007-Spring. IEEE 65th Vehicular Technology Conference*, Dublin, 2007.

[101] S. Salsano, L. Veltri, G. Martiniello and A. Polidoro, "Seamless vertical handover of VoIP calls based on SIP Session Border Controllers," in *IEEE International Conference on Communications*, Istanbul, 2006.

[102] R. Tawil, G. Pujolle and O. Salazar, "A Vertical Handoff Decision Scheme in Heterogeneous Wireless Systems," in *IEEE Vehicular Technology Conference*, Singapore, 2008.

[103] W. H. Yang, Y. C. Wang, Y. C. Tseng and B. S. P. Lin, "An Energy-Efficient Handover Scheme with Geographic Mobility Awareness in WiMAX-WiFi Integrated Networks," in *IEEE Wireless Communications and Networking Conference*, Budapest, 2009.

[104] M. Kassar, B. Kervella and G. Pujolle, "An overview of vertical handover decision strategies in heterogeneous wireless networks," *Computer Communications,* vol. 31, no. 10, p. 2607–2620, 2008.

[105] FMCA, "Addressing the Need for Inter-Access Seamless Mobility," FMCA, 5-7 October 2009. [Online]. Available: http://www.etsi.org/plugtests/FMCA09/FMCA.htm.

[106] Total Telecom, "FMCA successfully tests seamless mobility using the IEEE 802.21 standard," Total telecom, 23 October 2009. [Online]. Available: http://www.totaltele.com/view.aspx?ID=450108.

[107] D. Corujo, "ODTONE: An Open Source Multi-Platform Implementation of the IEEE 802.21 Protocol," 2010. [Online]. Available: http://atnog.github.io/ODTONE/.

[108] D. Corujo, C. Guimaraes, B. Santos and R. L. Aguiar, "Using an open-source IEEE 802.21 implementation for network-based localized mobility management," *Communications Magazine, IEEE .,* vol. 49, no. 9, pp. 114 - 123, 2011.

[109] Interdigital, "InterDigital Demonstrates Media Independent Handover (MIH) Technology at Mobile World Congress, Barcelona," Interdigital, 2009. [Online]. Available: http://ir.interdigital.com/common/mobile/iphone/releasedetail.cfm?ReleaseID=365692&CompanyID=IDCC&mobileid=.

[110] O. Fatokun and s. D. Y. Yang, “THE INVESTIGATION OF SIP BASED IEEE 802.21 MIH SIGNALLING FOR VERTICAL HANDOVER,” UCL, London UK, August 2009.

[111] A. Rahmati, A. Qian and L. Zhong, “Understanding human-battery interaction on mobile phones,” in *9th international conference on Human computer interaction with mobile devices and services*, New York, 2007.

[112] M.-S. Kim and S. Lee, “Load balancing based on layer 3 and IEEE 802.21 frameworks in PMIPv6 networks,” in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Tokyo, 2009.

[113] J.-M. Chung, D. Lee, W. Song, S. Choi, C. Lim and T. Yeoum, “Enhancements to FPMIPv6 for improved seamless vertical handover between LTE and heterogeneous access networks,” *Wireless Communications, IEEE,* vol. 20, no. 3, pp. 112 - 119, 2013.

[114] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, K. Redon, N. Golde and R. Borgaonkar, “New Privacy Issues in Mobile Telephony:Fix and Verification,” *CCS,* October 2012.

[115] Y. Park and T. Park, “A Survey of Security Threats on 4G Networks,” in *IEEE Globecom Workshops*, Washington, DC, 2007.

[116] I. Bilogrevic, M. Jadliwala and J.-P. Hubaux, “Security Issues in Next Generation Mobile Networks: LTE and Femtocells,” Luton, 2010.

[117] IEEE, "802.1X-2010," IEEE, 2010. [Online]. Available: http://standards.ieee.org/findstds/standard/802.1X-2010.html.

[118] O2, “iPhone business super user,” O2, 2010. [Online]. Available: http://www.o2.co.uk/sme/businesstariffs/tariffsforupto10people/iphonebusinesssuperuser/tariffbreakdown .

[119] B. Wifi, “News and press releases,” BT plc, 14 May 2013. [Online]. Available: https://www.btwifi.co.uk/news/news_20130514.jsp.

[120] IEEE, “IEEE 802.21 standard,” IEEE, 2008. [Online]. Available: http://www.ieee802.org/21/.

[121] N. Aleisa, “A Comparison of the 3DES and AES Encryption Standards,” *International Journal of Security and Its Applications,* vol. 9, no. 7, 2015.

[122] A. Patil and R. Goudar, “A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices,” *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH,* vol. 2, no. 8, 2013.

[123] D. Holmes and M. Santos, “Method and system for registering and verifying the identity of wireless networks and devices”. WO Patent WO 2008095291 A1 /CA2677362A1/EP2111704A1/US20100106966, 14 April 2008.

[124] R. Whelan, W. Lamar Van and R. Morris, “Managed roaming for wlans”. WO Patent EP1527563A2, US7606242, US20040198220, WO2004014024A3, 12 February 2004.

[125] V. K. Choyi, F. Gariador and A. Robison, “Mechanism for detection of attacks based on impersonation in a wireless network”. US/Eu/De Patent DE602004016272D1, EP1542406A2, EP1542406B1, US7409715, US20050144544, 9 November 2005.

[126] R. A. Khan and A. H. Mir, “IPsec in Mobile IP: A Survey,” *Network,* vol. 4, p. 6, 2012.

[127] 3GPP, “LTE;Evolved Universal Terrestrial Radio Access Network (E-UTRAN);X2 general aspects and principles,” November 2008.

[128] STOKE Inc., “SSX 3000,” Stoke Inc., [Online]. Available: http://www.stoke.com/products/ssx-3000.asp.

[129] A. Ulvan, R. Bestak and M. Ulvan, “The study of handover procedure in LTE-based femtocell network,” in *Wireless and Mobile Networking Conference (WMNC), 2010 Third Joint IFIP*, Budapest, 2010.

[130] A. Vakali and G. Pallis, “Content delivery networks: status and trends,” *IEEE Internet Computing,* vol. 7, no. 6, pp. 1089-7801, 2003.

[131] A.-M. K. Pathan and R. Buyya, “A Taxonomy and Survey of Content Delivery Networks,” 2007. [Online]. Available: http://www.hit.bme.hu/~jakab/edu/litr/CDN/CDN-Taxonomy.pdf. [Accessed 2014].

[132] S. Borst, V. Gupta and A. Walid, “Distributed Caching Algorithms for Content Distribution Networks,” in *Proceedings IEEE INFOCOM*, San Diego, CA, 2010.

[133] Saguna, “Deliver More for Less,” Saguna, [Online]. Available: http://www.saguna.net/solutions/deliver-more-for-less/. [Accessed 24 September 2014].

[134] Saguna Networks, “Saguna Networks Nominated for GSMA Award,” Saguna, 2012. [Online]. Available: http://www.saguna.net/news-events/press-releases/saguna-networks-nominated-for-gsma-award/. [Accessed 17 August 2014].

[135] Saguna - Intel, “Saguna Networks enables Mobile Network Operators to Monetize their Radio Networks,” 2013. [Online]. Available: http://www.saguna.net/site/assets/files/1/intel_saguna_networks_whitepaper.pdf. [Accessed august 2014].

[136] ETSI, “3GPP TS 23.401 General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access,” January 2015. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/123400_123499/123401/10.13.00_60/ts_123401v101300p.pdf. [Accessed February 2015].

[137] K. Wansink, P. Budde, P. Evans, H. Lancaster and p. Lange, “Global Broadband - Demand for Fibre Networks Grows,” budde.com, June 2014. [Online]. Available: http://www.budde.com.au/Research/Global-Broadband-Demand-for-Fibre-Networks-Grows.html#execsummary. [Accessed 21 October 2014].

[138] K. Smith, “Onboard connection: Operators strive to keep up with demand for train Wi-Fi,” International Railway Journal, 21 July 2014. [Online]. Available: http://www.railjournal.com/index.php/telecoms/onboard-connection-operators-strive-to-keep-up-with-demand-for-train-wi-fi.html. [Accessed 2014].

[139] C. Mullie, “Why is it Important to be Online and Underground?,” New Cities Foundation, 28 July 2014. [Online]. Available: http://www.newcitiesfoundation.org/why-is-it-important-to-be-online-and-underground/. [Accessed 2014].

[140] Aircraft Commerce, “Aircraft eEnablement Connectivity & IFE Conference,” Aircraft Commerce, 1-2 October 2014. [Online]. Available: http://www.aircraft-commerce.com/conferences/eEnablement2014/Homepage.asp. [Accessed 20 October 2014].

[141] R. Obermann, “Digital Minds for a New Europe- The Gigabit Gap and some thoughts on how to bridge it,” Vice-President Neelie Kroes, European Commissioner for the Digital Agenda for Europe, 2014. [Online]. Available: https://ec.europa.eu/commission_2010-2014/kroes/en/content/gigabit-gap-and-some-thoughts-how-bridge-it-ren%C3%A9-obermann. [Accessed October 2014].

[142] Sugarnet, "Sugarnet," Sugarnet, 2012. [Online]. Available: http://www.sugarnet.co.uk/. [Accessed 12 June 2013].

[143] Rural Broadband Partnership, "Rural Broadband Partnership," Rural Broadband Partnership, 2011. [Online]. Available: http://www.ruralbroadband.com/. [Accessed 9 August 2012].

[144] UKBroadband, "Rural Solutions," UKBroadband, 2012. [Online]. Available: http://www.ukbroadband.com/public-sector/rural-solutions. [Accessed 10 July 2013].

[145] A. Balasubramanian, R. Mahajan, A. Venkataramani, B. N. Levine and J. Zahorjan, "Interactive wifi connectivity for moving vehicles," in *ACM SIGCOMM*, Seattle, 2008.

[146] A. Balasubramanian, R. Mahajan and A. Venkataramani, "Augmenting mobile 3G using WiFi," in *8th international conference on Mobile systems, applications, and services*, San Francisco, 2010.

[147] W. v. Brussel, "Bringing ICT services to trains technical and economical challenges," in *9th Conference on Telecommunications Internet and Media Techno Economics (CTTE)*, Ghent, 2010.

[148] R. Morgenstern, "Spectrum demand for air/ground air traffic management communications," in *Integrated Communications, Navigation and Surveillance Conference*, Bethesda, 2008.

[149] S. Higginbotham, "Why your in-flight Wi-Fi is slow and expensive: It's all about the pipe," Gigaom, 19 September 2012. [Online]. Available: https://gigaom.com/2012/09/19/why-your-in-flight-wi-fi-is-slow-and-expensive-its-all-about-the-pipe/. [Accessed 14 August 2014].

[150] Deutsche Telekom, "https://www.telekom.com/media/company/107626," Deutsche Telekom, 15 March 2012. [Online]. Available: https://www.telekom.com/media/company/107626. [Accessed 13 July 2014].

[151] CEPT ECC, "FM 48 - Spectrum Aspects Broadband DA2GC Systems," CEPT ECC, [Online]. Available: http://www.cept.org/ecc/groups/ecc/wg-fm/fm-48/page/terms-of-reference.

[152] BT plc, “The BT Story,” BT plc, February 2015. [Online]. Available: http://www.btplc.com/Thegroup/Ourcompany/TheBTstory/index.htm. [Accessed 4 March 2015].

[153] Openreach, “Broadband Enabling Technology,” 2010. [Online]. Available: http://www.openreach.co.uk/orpg/home/products/llu/broadbandenablingtechnology/bet/downloads/BET_factsheet%202010-11-08%20pm.pdf.

[154] GMW software, “JD's Automatic Speed tester,” GMW software, [Online]. Available: http://www.gmwsoftware.co.uk/.

[155] ETSI Technical Committee Electromagnetic compatibility and Radio spectrum Matters, “ETSI TR 103 108: Electromagnetic compatibility and Radio spectrum Matters (ERM); System Reference document (SRdoc); Broadband Direct-Air-to-Ground Communications System operating in the 5,855 GHz to 5,875 GHz band using 3G technology,” ETSI, Sophia Antipolis, 2013.

[156] Aero3G, “SE44 050: Methodology for Generic Ground Station EIRP in the band 5,855 GHz to 5,875 GHz,” CEPT ECC, Copenhague, 2012.

[157] Aero3G, “SE44 053 Methodology for Generic Spurious/Out of Band Emissions Mask in the band 5,855 GHz to 5,875 GHz,” CEPT, Copenhague, 2012.

[158] S. Jones, “www.cambridgewireless.co.uk/,” 6th December 2012. [Online]. Available: http://www.cambridgewireless.co.uk/Presentation/Radio%20Tech%20SIG%2006.12.12%20ISM4G%20Frequency%20Domain%20Coexistence%20in%20Mobile%20Platforms.pdf. [Accessed 2013].

[159] N. Rupasinghe, “3GPP workshop - LTE in unlicensed spectrum,” Dept. of Electrical and Computer Engineering, Florida International University, Florida, 2014.

[160] L. Wan, “LTE-based Unlicensed Carrier Offloading,” Huawei, 2014.

[161] M. Jackson, “Ofcom Shun WiFi Interference Fears to Prep 2.3GHz Auction for Mobile,” ISPreview, 19 February 2014. [Online]. Available: http://www.ispreview.co.uk/index.php/2014/02/ofcom-shun-wifi-interference-concerns-auction-2-3ghz-mobile.html. [Accessed 12 August 2014].

[162] Y. T. Lin and K. C. Chen, “Co-existence studies of LTE-A with Carrier Aggregation at 3.5GHz band,” in *8th International Wireless Communications and Mobile Computing Conference*, Limassol, 2012.

[163] V. Krizanovic, D. Zagar and G. Martinovic, “Mobile broadband access networks planning and evaluation using techno-economic criteria,” in *34th International Conference on Information Technology Interfaces* , Cavtat, Dubrovnik, 2012.

[164] Y. S. Jeong, S. H. Lee, J. H. Yoon, W. Y. Lee, W. Y. Choi and Y. J. Yoon, “Internal mobile antenna for LTE / GSM850 / GSM900 / PCS1900 / WiMAX / WLAN,” in *IEEE Radio and Wireless Symposium*, New Orleans, LA, 2010.

[165] T. Nakamura, S. Nagata, A. Benjebbour, Y. Kishiyama, T. Hai, S. Xiaodong, Y. Ning and L. Nan, “Trends in small cell enhancements in LTE advanced,” *IEEE Communications Magazine ,* vol. 51, no. 2, pp. 98 - 105, 2013.

[166] V. Krizanovic, D. Zagar and K. Grgic, “Techno-economic analyses of wireline and wireless broadband access networks deployment in Croatian rural areas,” in *11th International Conference on Telecommunications*, Graz, 2011.

[167] A. Z. Yonis, M. F. L. Abdullah and M. F. Ghanim, “LTE-FDD and LTE-TDD for Cellular Communications,” in *Progress In Electromagnetics Research Symposium Proceedings,*, Kuala Lumpur, 2012.

[168] TriQuint, “LTE / Wi-Fi coexistence filter,” September 2013. [Online]. Available: http://www.triquint.com/products/d/triquint-wi-fi-coexist-filters-brochure. [Accessed 22 October 2013].

[169] “http://www.huawei.com/ilink/en/download/HW_204545,” February 2013. [Online]. Available: http://www.huawei.com/ilink/en/download/HW_204545. [Accessed June 2013].

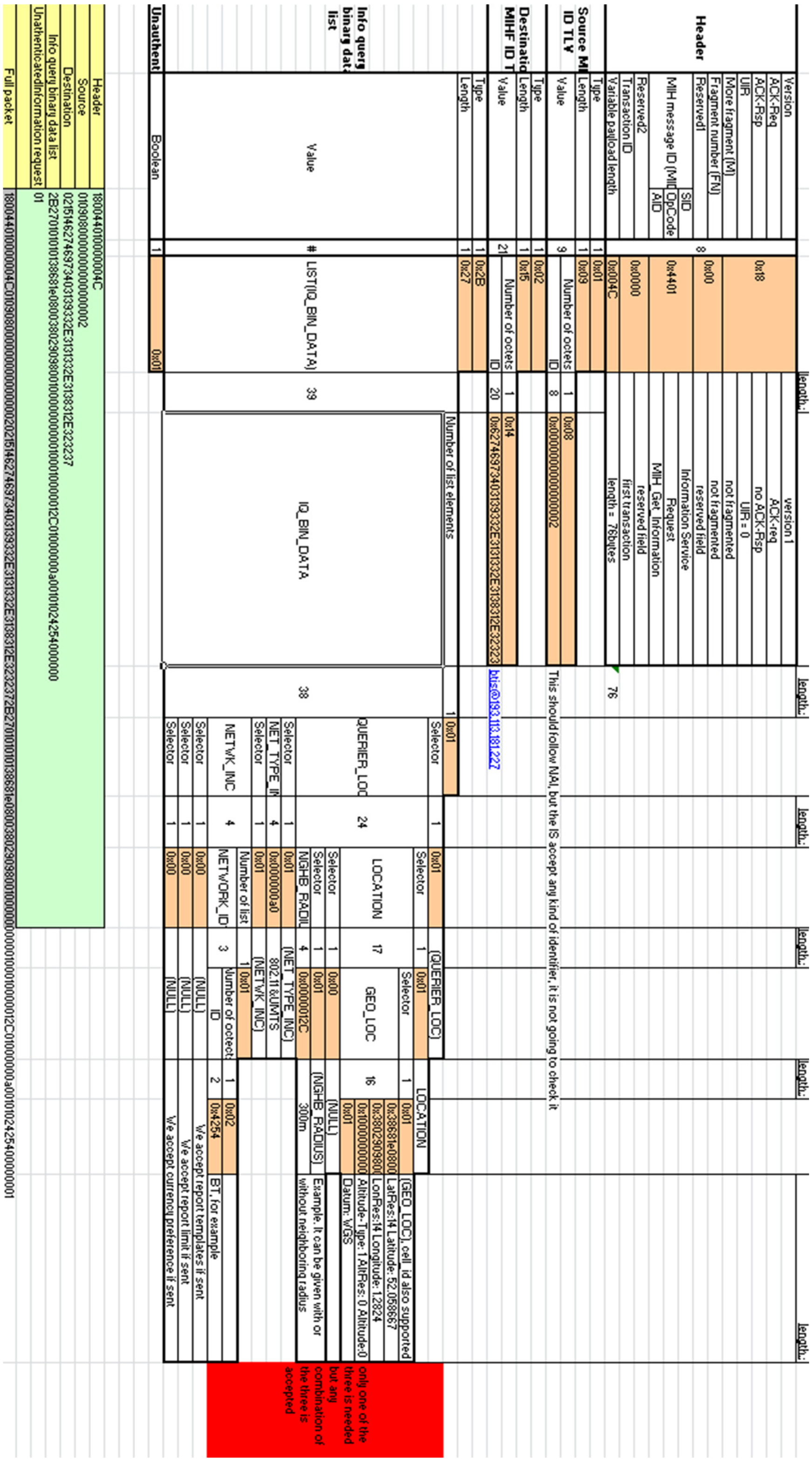
[170] Ofcom, “7th DRAFT Co-existence and Co-ordination Guidelines for FWA at 3.4 – 3.6 GHz,” Ofcom, London, 2012.

[171] D. Crosby, V. S. Abhayawardhana, I. J. Wassell, M. G. Brown and M. P. Sellars, “Time variability of the foliated fixed wireless access channel at 3.5 GHz,” in *2005 IEEE 61st Vehicular Technology Conference*, 2005.

[172] K. Lee, J. Lee, Y. Yi, I. Rhee and S. Chong, “Mobile data offloading: how much can WiFi deliver?,” in *Co-NEXT '10*, New York, 2010.

Annex A: 802.21 MIH Messages

See below an example of a client request to MIIS



					length:		length:		length:		length:		length:		length:	
Header	Version		8	0x18	version 1											
	ACK-Req				ACK-req											
	ACK-Rsp				no ACK-Rsp											
	UIR				UIR = 0											
	More fragment (M)				not fragmented											
	Fragment number (FN)			0x00	not fragmented											
	Reserved1				reserved field											
	MIH message ID (MII	SID		0x4401	Information Service											
		OpCode			Request											
		AID			MIH_Get_Information											
	Reserved2			0x0000	reserved field											
	Transaction ID				first transaction											
	Variable payload length			0x004C	length = 76bytes	76										
Source MI ID TLV	Type		1	0x01												
	Length		1	0x09												
	Value		9	Number of octets	1	0x08										
				ID	8	0x0000000000000002	This should follow NAI, but the IS accept any kind of identifier, it is not going to check it									
Destinatio MIHF ID T	Type		1	0x02												
	Length		1	0x15												
	Value		21	Number of octets	1	0x14										
				ID	20	0x62746973403139332E3131332E3138312E32323	btis@193.113.181.227									
Info query binary data list	Type		1	0x2B												
	Length		1	0x27												
	Value		#	LIST(IQ_BIN_DATA)	39	Number of list elements	1	0x01								
						IQ_BIN_DATA	38	Selector	1	0x01	(QUERIER_LOC)					only one of the three is needed but any combination of the three is accepted
								QUERIER_LOC	24	Selector	1	0x01	LOCATION			
										LOCATION	17	Selector	1	0x01	(GEO_LOC), cell_id also supported	
												GEO_LOC	16	0x38681e0800	LatRes:14 Latitude: 52.058667	
														0x3802909800	LonRes:14 Longitude: 1.2824	
														0x1000000000	Altitude-Type: 1 AltRes: 0 Altitude:0	
														0x01	Datum: WGS	
										Selector	1	0x00	(NULL)			
										Selector	1	0x01	(NGHB_RADIUS)		Example. It can be given with or without neighboring radius	
										NGHB_RADIU	4	0x0000012C	300m			
								Selector	1	0x01	(NET_TYPE_INC)					
								NET_TYPE_IN	4	0x000000a0	802.11 &UMTS					
								Selector	1	0x01	(NETWK_INC)					
								NETWK_INC	4	Number of list	1	0x01				
										NETWORK_ID	3	Number of octects	1	0x02		
												ID	2	0x4254	BT, for example	
								Selector	1	0x00	(NULL)	We accept report templates if sent				
								Selector	1	0x00	(NULL)	We accept report limit if sent				
								Selector	1	0x00	(NULL)	We accept currency preference if sent				
Unauthent	Boolean		1	0x01												

Header	180044010000004C
Source	01090800000000000000002
Destination	021514627469734031393332E3131332E3138312E323237
Info query binary data list	2B270101010138681e0800380290980010000000000100010000012C01000000a00101024254000000
UnathenticatedInformation request	01
Full packet	180044010000004C01090800000000000000002021514627469734031393332E3131332E3138312E3232372B270101010138681e0800380290980010000000000100010000012C01000000a0010102425400000001

Table 25 - Typical MIH client information request with GPS coordinates.

See below a typical response from the MIIS service

Section	Field	Length	Value / Sub-field	Length	Value	Description
Header	Version	8	0x14			version 1
	ACK-Req					ACK-req
	ACK-Rsp					ACK-Rsp
	UIR					UIR = 0
	More fragment (M					not fragmented
	Fragment number (		0x00			not fragmented
	Reserved1					reserved field
	MIH mes SID		0x4801			Information Service
	OpCode					Response
	AID					MIH_Get_information
	Reserved2		0x0001			reserved field
	Transaction ID					first transaction
	Variable payload le		0x0029			length = 41 bytes
Source ID TLV	Type	1	0x01			
	Length	1	0x15			
	Value	21	Number of octets	1	0x14	
			ID	20	0x6274697340313933 2E3131	btis@193.113.181.227
Destina MIHF II	Type	1	0x02			
	Length	1	0x09			
	Value	9	Number of octets	1	0x08	
			ID	8	0x0000000000000002	
tatus TL	Type	1	0x03			
	Length	1	0x01			
	Value	1	STATUS	1	0x00	(Success)
Info Re Binary Data Li	Type	1	0x30			Type = 48
	Length	2	0x8112			Length = 146
	LIST(IR_BIN_DATA	147	umber of list elements	1	0x01	Number of IR_BIN_DATA
			INFO_ELEMENT (145) – Number of list element	1	0x01	Number of INFO_ELEMENTS

Element	Length	Field	Length	Value	Description
CONTAINER_LIST_OF_NETW (145)		Type	4	0x10000300	
		Length	2	0x810b	
IE_CONTAINER_NETWORK	139	Type	4	0x1000301	
		Length	2	0x8105	
IE_NETWORK_TYPE	9	Type	4	0x10000000	
		Lenght	1	0x04	
		Selector	1	0x01	(LINK_TYPE)
		LINK_TYPE	1	0x13	802.11
		Selector	1	0x00	(NULL) no info on database about subtype, could be added later
		Selector	1	0x00	(NULL) no very useful
IE_OPERATOR_ID	9	Type	4	0x10000001	
		Length	1	0x04	
		OP_NAME (3) – Number of octec	1	0x02	
		Value	2	0x4254	BT
		OP_NAMESPAC	1	0x03	ITU/TSB
IE_NETWORK_ID	13	Type	4	0x10000100	
		Length	1	0x04	
		Number of octect	1	0x07	
		Value	7	0x504943547572	PICTURE
IE_COST	12	Type	1	0x10000103	
		Length	1	0x0a	
		COST_UNIT	1	0x07	
		COST_VALUE (6) – INTEGER PART	4	0x00000000	
		FRACTION PAF	2	0x0000	
		COST_CURR	3	0x474250	GBP
IE_NETWORK_DATA_RATE	6	Type	1	0x10000106	
		Length	1	0x04	
		value	4	0x00001800	6144kbps
E_CONTAINER_POA	84	Type	1	0x10000302	
		Length	1	0x04	
IE_POA_LINK_ADDR	15	Type	4	0x10000200	
		Length	1	0x0a	
LINK_ADDR	10	Selector	1	0x00	(MAC_ADDR)
MAC_ADDR	9	Type	2	0x0006	
Value	7	Number (	1	0x06	
		MAC_AD	6	0x623835623966	
IE_POA_LOCATION	22	Type	4	0x10000201	
		Length	1	0x11	
LOCATION	17	Selector	1	0x01	(GEO_LOC), cell_id also supported
GEO_LOC	16			0x38681e080(	LatRes:14 Latitude: 52.058667
				0x380290980	LonRes:14 Longitude: 1.2824
				0x100000000(	Altitude-Type: 1 AltRes: 0 Altitude:0 m
				0x01	Datum: WGS
IE_POA_CHANNEL_RANGE	13	Type	4	0x10000202	
		Length	1	0x08	
		lower freq	4	0x00250490	2.426 GHz
		upper freq	4	0x00255a80	2.448 GHz
IE_POA_SYSTEM_INFO	20	Type	4	0x10000203	
		Length	1	0x0e	
NETWORK_TYPE	4	Selector	1	0x01	(LINK_TYPE)
		LINK_TYPE	1	0x13	802.11
		Selector	1	0x00	(NULL) no info on database about subtype, could be added later
		Selector	1	0x00	(NULL) not very useful
LINK_ADDR	10	Selector	1	0x00	(MAC_ADDR)
MAC_ADDR	9	Type	2	0x0006	
Value	7	Number (	1	0x06	
		MAC_AD	6	0x623835623966	
		Selector	1	0x00	(NULL)
IE_POA_SUBNET_INFO	12	Type	4	0x10000203	
		Length	1	0x07	
P_SUBNET_INFO	7	IP_PREFIX	1	0x18	
IP_ADDR			2	0x01	
			4	0xc171b501	

Header	1400480100010029
Source	0115146274697340313933 2E3131332E3138312E323237
Destination	020908000000000000000002
Status	030100
response binary dat	308112010110000300810b10003018105100000000401130000100000010402425403100001000407504943547572651000010 30a070000000000000474250100001 06
	040000180010000302041000020 00a000006066238356239661000020111013868 1e080038029098001000000000011000020208002504900025 5a80100002030e0113000000000606
	623835623966001000020307180 1c171b501
Full packet	14004801000100290115146274697340313933 2E3131332E3138312E3232370209080000000000000000020301003081120101100003 00 810b10003018105100000000401130000100000010402425403100001000407504943547572651000010 30a0700000000000004742501000010604000018001000030204100002000a00000606623835623966100002011101386 81e080038029098001000000000110000 2020800250490002 55a80100002030e0113000000000606

Table 26 - MIIS typical response to an information request.

		length.:		length.:		length.:		length.:		length.:		length.:		length.:	
Header	Version	8	0x10	version 1											
	ACK-Req			no ACK-req											
	ACK-Rsp			no ACK-Rsp											
	UIR			UIR = 0											
	More fragment (M)		0x00	not fragmented											
	Fragment number (FN)			not fragmented											
	Reserved1			reserved field											
	MIH message ID (MID): SID		0x3403	Command Service											
	MIH message ID (MID): OpCode			Request											
	MIH message ID (MID): AID			MIH_Link_Actions											
	Reserved2		0x0000	reserved field											
	Transaction ID			first transaction											
	Variable payload length		0x0029	length = 41 bytes											
Source MIHF ID TLV	Type	1	0x01												
	Length	1	0x09												
	Value	9	Number of octets	1	0x08										
			ID	8	0x0000000000000001										
Destination MIHF ID TLV	Type	1	0x02												
	Length	1	0x09												
	Value	9	Number of octets	1	0x08										
			ID	8	0x0000000000000002										
Link Action List TLV	Type	1	0x27	type = 39											
	Length	1	0x11	length = 17											
	Value	17	Number of list elements	1	0x01										
			LINK_ACTION_REQ	16	LINK_ID	11	LINK_TYPE	1	0x1B	(WiMax)					
							LINK_ADDR	10	(MAC_ADDR)	9	Selector	1	0x00	(MAC_ADDR)	
											Type	2	0x0006		
											Value	7	Number of octets	1	0x06
													MAC_ADDR	6	0x000000000001
					Selector	1	0x00	(NULL)							
					LINK_ACTION	2	LINK_AC_TYPE	1	0x04	(LINK_POWER_UP)					
							LINK_AC_ATTR	1	0x01	(LINK_SCAN)					
					LINK_AC_EX_TIME	2	0x0000	(0 ms)							

Header	1000340300000029
Source	0109080000000000000001
Destination	0209080000000000000002
Link Action List part 1	2711011B000006060000000000010004010000
Full packet	1000340300000029010908000000000000000102090800000000000000022711011B000006060000000000010004010000

Table 27 - MICS request to power up WiMAX.

		length.:		length.:		length.:		length.:		length.:		length.:		length.:	
Header	Version	8	0x10	version 1											
	ACK-Req			no ACK-req											
	ACK-Rsp			no ACK-Rsp											
	UIR			UIR = 0											
	More fragment (M)		0x00	not fragmented											
	Fragment number (FN)			not fragmented											
	Reserved1			reserved field											
	MIH message ID (MID): SID		0x3803	Command Service											
	MIH message ID (MID): OpCode			Response											
	MIH message ID (MID): AID			MIH_Link_Actions											
	Reserved2		0x0000	reserved field											
	Transaction ID			first transaction											
	Variable payload length		0x003F	length = 63 bytes											
Source MIHF ID TLV	Type	1	0x01												
	Length	1	0x09												
	Value	9	Number of octets	1	0x08										
			ID	8	0x0000000000000002										
Destination MIHF ID TLV	Type	1	0x02												
	Length	1	0x09												
	Value	9	Number of octets	1	0x08										
			ID	8	0x0000000000000001										
Status TLV	Type	1	0x03												
	Length	1	0x01												
	Value	1	STATUS	1	0x00	(Success)									
Link Action Result List TLV	Type	1	0x28	Type = 40											
	Length	1	0x1D	Length = 29											
	Value	36	Number of list elements	1	0x01										
			LINK_ACTION_RES	35	LINK_ID	11	LINK_TYPE	1	0x1B	(WiMax)					
							LINK_ADDR	10	(MAC_ADDR)	9	Selector	1	0x00	(MAC_ADDR)	
											Type	2	0x0006		
											Value	7	Number of octets	1	0x06
													MAC_ADDR	6	0x000000000001
					LINK_AC_RESULT	1	0X00	(Success)							
					Selector	1	0x01	(LIST(LINK_SCAN_RSP))							
					Number of list elements	1	0x01	(1 element)							
					LINK_SCAN_RSP	21	LINK_ADDR	10	(MAC_ADDR)	9	Selector	1	0x00	(MAC_ADDR)	
											Type	2	0x0006		
											Value	7	Number of octets	1	0x06
													MAC_ADDR	6	0x000000000010
							NETWORK_ID	9	Number of octets	1	0x01				
									ID	8	0x0000000000000001				
							SIG_STRENGTH	2	Selector	1	0x01	(INTEGER)			
									(Absolute singal strength)	1	0x64	(100 dBm)			

Header	100038030000003F
Source	0109080000000000000002
Destination	0209080000000000000001
Status	030100
Link Action List part 1	281D011B000006060000000000000100010100
Link Action List part 2	00060600000000000100100000000000000010164
Full packet	100038030000003F01090800000000000000020209080000000000000001030100281D011B000006060000000000000100010100 00060600000000000100100000000000000010164

Table 28 - MICS WiMAX scan results response.

TLV	Field	Length	Value	Description
Header	Version	8	0x10	version 1
	ACK-Req			no ACK-req
	ACK-Rsp			no ACK-Rsp
	UIR			UIR = 0
	More fragment (M)		0x00	not fragmented
	Fragment number (FN)			not fragmented
	Reserved1			reserved field
	MIH message ID (MID) > SID		0x3403	Command Service
	MIH message ID (MID) > OpCode			Request
	MIH message ID (MID) > AID			MIH_Link_Actions
	Reserved2		0x0000	reserved field
	Transaction ID			first transaction
	Variable payload length		0x0033	length = 51 bytes
Source MIH ID TLV	Type	1	0x01	
	Length	1	0x09	
	Value (9) > Number of octets	1	0x08	
	Value (9) > ID	8	0x0000000000000001	
Destination MIHF ID TLV	Type	1	0x02	
	Length	1	0x09	
	Value (9) > Number of octets	1	0x08	
	Value (9) > ID	8	0x0000000000000002	
Link Action List TLV	Type	1	0x27	type = 39
	Length	1	0x11	length = 17
	Value (27) > Number of list elements	1	0x01	
	Value (27) > LINK_ACTION_REQ (26) > LINK_ID (11) > LINK_TYPE	1	0x1B	(WiMax)
	Value (27) > LINK_ACTION_REQ (26) > LINK_ID (11) > LINK_ADDR (#) > Selector	1	0x00	(MAC_ADDR)
	Value (27) > LINK_ACTION_REQ (26) > LINK_ID (11) > LINK_ADDR (#) > (MAC_ADDR) (9) > Type	2	0x0006	
	Value (27) > LINK_ACTION_REQ (26) > LINK_ID (11) > LINK_ADDR (#) > (MAC_ADDR) (9) > Value (7) > Number of octets	1	0x06	
	Value (27) > LINK_ACTION_REQ (26) > LINK_ID (11) > LINK_ADDR (#) > (MAC_ADDR) (9) > Value (7) > MAC_ADDR	6	0x000000000001	
	Value (27) > LINK_ACTION_REQ (26) > Selector	1	0x01	(LINK_ADDR)
	Value (27) > LINK_ACTION_REQ (26) > LINK_ADDR (10) > Selector	1	0x00	(MAC_ADDR)
	Value (27) > LINK_ACTION_REQ (26) > LINK_ADDR (10) > (MAC_ADDR) (9) > Type	2	0x0006	
	Value (27) > LINK_ACTION_REQ (26) > LINK_ADDR (10) > (MAC_ADDR) (9) > Value (7) > Number of octets	1	0x06	
	Value (27) > LINK_ACTION_REQ (26) > LINK_ADDR (10) > (MAC_ADDR) (9) > Value (7) > MAC_ADDR	6	0x000000000010	
	Value (27) > LINK_ACTION_REQ (26) > LINK_ACTION (2) > LINK_AC_TYPE	1	0x04	(LINK_POWER_UP)
	Value (27) > LINK_ACTION_REQ (26) > LINK_ACTION (2) > LINK_AC_ATTR	1	0x00	(NONE)
	Value (27) > LINK_ACTION_REQ (26) > LINK_AC_EX_TIME	2	0x0000	(0 ms)

Header	1000340300000033
Source	01090800000000000000001
Destination	02090800000000000000002
Link Action List part 1	2711011B000006060000000000000101000006060000000000001004000000
Full packet	100034030000003301090800000000000000001020908000000000000000022711011B000006060000000000000101000006060000000000001004000000

Table 29 - MICS WiMAX connect request.

TLV	Field	Length	Value	Description
Header	Version	8	0x10	version 1
	ACK-Req			no ACK-req
	ACK-Rsp			no ACK-Rsp
	UIR			UIR = 0
	More fragment (M)		0x00	not fragmented
	Fragment number (FN)			not fragmented
	Reserved1			reserved field
	MIH message ID (MID) > SID		0x3803	Command Service
	MIH message ID (MID) > OpCode			Response
	MIH message ID (MID) > AID			MIH_Link_Actions
	Reserved2		0x0000	reserved field
	Transaction ID			first transaction
	Variable payload length		0x0052	length = 82 bytes
Source MIHF ID TLV	Type	1	0x01	
	Length	1	0x09	
	Value (9) > Number of octets	1	0x08	
	Value (9) > ID	8	0x0000000000000002	
Destination MIHF ID TLV	Type	1	0x02	
	Length	1	0x09	
	Value (9) > Number of octets	1	0x08	
	Value (9) > ID	8	0x0000000000000001	
Status TLV	Type	1	0x03	
	Length	1	0x01	
	Value (1) > STATUS	1	0x00	(Success)
Link Action Result List TLV	Type	1	0x28	Type = 40
	Length	1	0x1D	Length = 29
	Value (36) > Number of list elements	1	0x01	
	Value (36) > LINK_ACTION_RES (35) > LINK_ID (11) > LINK_TYPE	1	0x1B	(WiMax)
	Value (36) > LINK_ACTION_RES (35) > LINK_ID (11) > LINK_ADDR (10) > Selector	1	0x00	(MAC_ADDR)
	Value (36) > LINK_ACTION_RES (35) > LINK_ID (11) > LINK_ADDR (10) > (MAC_ADDR) (9) > Type	2	0x0006	
	Value (36) > LINK_ACTION_RES (35) > LINK_ID (11) > LINK_ADDR (10) > (MAC_ADDR) (9) > Value (7) > Number of octets	1	0x06	
	Value (36) > LINK_ACTION_RES (35) > LINK_ID (11) > LINK_ADDR (10) > (MAC_ADDR) (9) > Value (7) > MAC_ADDR	6	0x000000000001	
	Value (36) > LINK_ACTION_RES (35) > LINK_AC_RESULT	1	0X00	(Success)
	Value (36) > LINK_ACTION_RES (35) > Selector	1	0x00	(NULL)
IP Address Link TLV	Type	1	0x65	
	Length	1	0x11	
	Value (17) > LINK_ID (11) > LINK_TYPE	1	0x1B	(WiMax)
	Value (17) > LINK_ID (11) > LINK_ADDR (10) > Selector	1	0x00	(MAC_ADDR)
	Value (17) > LINK_ID (11) > LINK_ADDR (10) > (MAC_ADDR) (9) > Type	2	0x0006	
	Value (17) > LINK_ID (11) > LINK_ADDR (10) > (MAC_ADDR) (9) > Value (7) > Number of octets	1	0x06	
	Value (17) > LINK_ID (11) > LINK_ADDR (10) > (MAC_ADDR) (9) > Value (7) > MAC_ADDR	6	0x000000000001	
	Value (17) > Type	1	0x01	(IPv4)
	Value (17) > Number of octets	1	0x04	
	Value (17) > IP Address	4	0x98440101	(152.68.1.1)

Header	1000380300000052
Source	01090800000000000000002
Destination	02090800000000000000001
Status	030100
Link Action List part 1	281D011B000006060000000000000100006511
Link Action List part 2	1B000006060000000000001010498440101
Full packet	10003803000000520109080000000000000000020209080000000000000000103010028 1D011B0000060600000000000001000065111B000006060000000000001010498440101

Table 30 - MICS WiMAX connected and IP TLV information.

Annex B: Measurements from 3.6GHz LTE TDD

	Cat	Description	DistanceFromBS_km	Lat	Long	altitude	Measure 1											Measure 2										
							height (m)	cellID	bars	SINR	RSSI	RSRP	RSRQ	Download (MB/s)	Upload(MB/s)	Download (Mbps)	Upload (Mbps)	height (m)	cellID	bars	SINR	RSSI	RSRP	RSRQ	Download	Upload	Download (Mbps)	Upload (Mbps)
1	b	Sutton, B1083, TVWS BS, "L" top	5.633	52.068126	1.362664	18	7	92	1	16	-84	-109	-12	2.19	0.509	17.52	4.07	3	92	1	4	-90	-123	-24	1.11	0.085	8.88	0.68
2	b	Sutton, The Plough car park, "L" mid	5.656	52.066422	1.363477	15	7	92	1	8	-89	-114	-12	1.75	0.109	14.00	0.87	3	92	0 -		-97	-132	-31	0.578	0	4.62	0.00
3	b	Sutton, off B1083, "L" mid	5.592	52.066287	1.362561	15	7	92	1	8	-90	-118	-14	1.56	0.0688	12.48	0.55	3									0.00	0.00
4	b	Sutton, Community Hall, "L" corner	5.784	52.062169	1.36614	15	7	92	2	16	-81	-107	-12	2.47	0.085	19.76	0.68	3	92	2	18	-83	-108	-12	1.8	0.0272	14.40	0.22
5	b	Sutton, Old Post Office Lane, "L" bottom	6.098	52.063923	1.370507		not available									0.00	0.00	*									0.00	0.00
6	r/b/n	B1083, between Sutton & Shottisham, pw7, no woods 300m away	6.248	52.057801	1.373109	6	7	92	2	14	-80	-107	-19	1.85	0.556	14.80	4.45	3	92	1	9	-93	-122	-16	1.18	0.232	9.44	1.86
7	r/b/n	B1083, between Sutton & Shottisham, pw6, with woods	6.366	52.055919	1.374745	3	8									0.00	0.00	*									0.00	0.00
8	b	Shottisham, Heath Drive, on hillside	7.175	52.050919	1.385919	19	8	92	2	14	-84	-117	-22	1.9	0.397	15.20	3.18	3	92	1	10	-89	-112	-15	1.37	0.263	10.96	2.10
9	n/b	Sutton, Melton Rd, open, 7km distance, on hill, pw108, out of coverag	6.844	52.085156	1.372066											0.00	0.00										0.00	0.00
10	r	Sutton, Haddon Approach, nearest point to river, valley	3.77	52.079881	1.324676											0.00	0.00										0.00	0.00
11	b	Sutton, Farm track, check under 25/5Mbps	4.562	52.082585	1.335877											0.00	0.00										0.00	0.00
12	r	Adastral, Hub, indoors wo antenna	0.105	52.058483	1.280207	25	8	91	5	19	-44	-76	-20	3.3	1.69	26.40	13.52	3	91	5	11	-48	-76	-17	3.05	1.48	24.40	11.84
13	r	Adastral, GDC Mobility area, indoors wo antenna	0.293	52.055987	1.281141	25	8									0.00	0.00										0.00	0.00
14	r	Adastral, road behind Orion, pw15	0.328	52.055745	1.280505	25	8	93	2	24	-70	-100	-16	4.4	1.3	35.20	10.40	3	93	3	26	-69	-93	-10	4.74	1.3	37.92	10.40
15	r	Adastral, road in front of Anteras, LOS, pw14	0.263	52.056561	1.279774	25	8	93	5	26	-44	-75	-21	6.17	1.36	49.36	10.88	3	93	5	28	-41	-69	-20	6.06	1.44	48.48	11.52
16	r	4-Acre, LOS past Orion, pw17	0.779	52.051607	1.281118	24										0.00	0.00										0.00	0.00
17	r	4-Acre, blocked by Orion, pw16	0.8	52.051607	1.278966	24	8	91	5	14	-48	-79	-21	3.37	1.34	26.96	10.72	3	93	3	7	-70	-101	-21	2.47	1.47	19.76	11.76
18	r	Brightwell, Ipswich Rd corner, pw109, clutter	1.007	52.050094	1.286772	25	9	93	3	10	-70	-101	-17	2.25	1.22	18.00	9.76	3									0.00	0.00
19	r	Martlesham Heath, Eagle Way, before buildings, pw20	0.638	52.061219	1.273433	26	8	91	4	26	-63	-93	-20	6.09	1.88	48.72	15.04	3	91	2	20	-77	-100	-16	4.99	1.14	39.92	9.12
20	r	Martlesham Heath, Eagle Way, behind buildings, pw19	0.743	52.06099	1.271587	27	8	91	5	35	-48	-72	-12	6.24	1.84	49.92	14.72	3	91	3	24	-74	-99	-12	6.23	1.8	49.84	14.40
21	r	Martlesham Heath, Eagle Way, no trees, pw22/23	0.458	52.056784	1.275713	24	8	93	5	11	-54	-80	-23	2.64	1.84	21.12	14.72	3	93	3	13	-68	-91	-18	2.39	1.51	19.12	12.08
22	r	Martlesham Heath, Eagle Way, behind trees, pw21/23	0.948	52.054942	1.269207	28	8	93	1	13	-85	-119	-26	1.94	0.229	15.52	1.83	3	93	1	9	-90	-124	-16	1.4	0.144	11.20	1.15
23	r	Changed to Martlesham Heath, Mayfield Lane, no trees, pw22/21	0.689	52.054895	1.273698	24	8	93	5	27	-44	-80	-23	6.06	1.84	48.48	14.72	3	93	5	25	-50	-76	-22	6.18	1.61	49.44	12.88
24	r	Martlesham Heath, Harvesters Way, behind some trees	1.147	52.057742	1.265017	26	8	93	3	12	-70	-99	-22	2.59	1.33	20.72	10.64	3	93	1	14	-84	-114	-11	2.12	0.522	16.96	4.18
25	r	Martlesham Heath, Forest Lane, behind more trees	0.916	52.057059	1.268571	26	8	93	4	23	-72	-99	-23	4.94	1.19	39.52	9.52	3	93	2	14	-78	-106	-17	2.32	0.655	18.56	5.24
26	r	Martlesham Heath, Dobbs Lane, even more trees, pw24/25	1.477	52.056667	1.260361	28	8	93	3	22	-55	-84	-12	5	1.63	40.00	13.04	3	93	2	14	-79	-103	-11	1.91	0.072	15.28	0.58
27	r	Kesgrave, Saint Isidores, more distant trees suburban, coverage	2.049	52.062087	1.252297	33	8	91	1	9	-85	-116	-17	1.21	0.38	9.68	3.04	3									0.00	0.00
28	r	Kesgrave, Dobbs Lane, pw29/30, no trees	1.519	52.063656	1.261092	31	8	91	5	18	-54	-81	-14	2.95	1.34	23.60	10.72	3	91	2	12	-80	-108	-14	2.11	0.435	16.88	3.48
29	r	Kesgrave, Dobbs Lane, trees	1.382	52.062153	1.262366	27	8	91	2	12	-79	-107	-15	2.73	1.25	21.84	10.00	3 no sig									0.00	0.00
30	r	Kesgrave, Dobbs Lane, no trees, more distance	1.705	52.066047	1.259922	35	8	91	4	25	-60	-85	-10	5	1.34	40.00	10.72	3	91	4	21	-66	-92	-12	5.29	1.37	42.32	10.96
31	r	Martlesham, A1214, Main Road, trees, main beam, pw32/33/34	1.772	52.068269	1.261127	33	8	91	4	26	-62	-88	-12	4.9	1.24	39.20	9.92	3	91	3	14	-82	-102	-15	3.86	1.28	30.88	10.24
32	r/b	Martlesham, Hall Road, more trees, main beam, pw31/33/34	1.91	52.07011	1.260989	85	8									0.00	0.00										0.00	0.00
33	n/b	Martlesham, Hall Road, pw31/32/34, no coverage	2.049	52.071654	1.260576											0.00	0.00										0.00	0.00
34	b/r	Martlesham, Hall Road, pw31/32/33	2.187	52.072776	1.259543											0.00	0.00										0.00	0.00
35	r	Kesgrave, Playford Road, clutter, pw36/37/38	3.153	52.074744	1.243812	38	8	91	1	10	-91	-112	-17	1.47	0.13	11.76	1.04	3	91	1	7	-89	-117	-10	1.33	0.143	10.64	1.14
36	r	Kesgrave, Playford Road, no clutter,1 tree in front when 8m, pw35/37	3.311	52.073467	1.239747	33	8	91	3	19	-72	-102	-24	4.21	1.57	33.68	12.56	3	91	3	19	-68	-99	-23	4.54	1.66	36.32	13.28
37	r/b	Kesgrave, Martlesham Road, clutter, pw36/35/38	2.732	52.078245	1.257719	25	8	91	1	4	-91	-125	-18	1.34	0.129	10.72	1.03	3	91	1	4	-95	-121	-18	1.53	0.141	12.24	1.13
38	r	Kesgrave, Playford Road, no clutter, pw36/37/35	4.139	52.071115	1.224707		*									0.00	0.00	*									0.00	0.00
39	r	Martlesham, Black Tiles Lane, trees pw110	1.432	52.070171	1.272542	33	8	91	3	19	-79	-102	-12	5.71	1.17	45.68	9.36	3	91	2	23	-73	-101	-11	5.6	1.14	44.80	9.12
40	r	Adastral, Road outside Car Park G, pw41/44, shadow effect from siriu	0.259	52.060783	1.280413	25	8	91	5	26	-45	-71	-21	5.06	1.27	40.48	10.16	3	91	5	26	-45	-78	-16	6.08	2.08	48.64	16.64
41	r	Adastral, Car Park G, pw40/44, shadow effect from sirius	0.222	52.060422	1.280413	25	8	91	5	29	-49	-69	-15	5.46	1.24	43.68	9.92	3	91	5	26	-47	-73	-21	6.18	1.38	49.44	11.04
43	r	Martlesham Heath, Hawker Drive, surrounded clutter industrial estate	0.486	52.062757	1.279538	25	8	91	5	32	-52	-74	-10	5.97	1.59	47.76	12.72	3	91	5	32	-48	-74	-11	6.06	1.87	48.48	14.96
44	r	Adastral, Car Park G, p w41/40, shadow effect from sirius	0.188	52.060175	1.280725	25	8	91	5	33	-38	-65	-15	6.17	2.09	49.36	16.72	3	91	5	26	-49	-82	-25	6.16	2.09	49.28	16.72
45	r	Adastral, Car Park U, close LoS	0.299	52.060114	1.285351	25	8	92	5	27	-55	-86	-24	6.01	1.5	48.08	12.00	3	92	5	27	-51	-83	-21	6.09	1.49	48.72	11.92
46	r	Adastral, Car Park S, behind Columba House, NLoS, pw48	0.207	52.058509	1.28475	25	8	93	5	23	-56	-80	-11	3.98	1.6	31.84	12.80	3	93	4	22	-58	-83	-9	3.44	1.69	27.52	13.52
48	r	Adastral, Car Park Z, pw46, no shadow	0.395	52.058285	1.287481	25	8	91	5	34	-50	-76	-11	6.09	1.32	48.72	10.56	3	91	5	33	-57	-83	-12	6.15	1.28	49.20	10.24
50	r	Test range clutter free, pw59	1.113	52.056736	1.297722	24										0.00	0.00										0.00	0.00
52	r	Car park B, Adastral, close behind trees	0.323	52.056137	1.284224	25	8	93	5	16	-54	-86	-23	2.6	1.4	20.80	11.20	3	91	5	27	-52	-81	-16	4.65	1.81	37.20	14.48
53	n	Xavi's house, just testing	7.591	52.053693	1.170996	30										0.00	0.00										0.00	0.00
54		Woodbridge road, urban 7km	6.789	52.061794	1.182562	44										0.00	0.00										0.00	0.00
55	n/b	Foxhall road, not spot, behind forest	4.324	52.049156	1.220391	34										0.00	0.00	no signal									0.00	0.00
56	n/b	Foxhall road, not spot, within forest	3.883	52.050159	1.226626	27										0.00	0.00	no signal									0.00	0.00
57	n/b/r	Bell Lane, Border, clutter free, pw58	3.304	52.051575	1.234776	35	8	93	3	21	-84	-94	-11	2.4	1.44	19.20	11.52	3	93	2	13	-80	-103	-12	2	1.38	16.00	11.04
58	r/b	Bell Lane, Border, clutter free, pw57	3.287	52.053738	1.23431	35	8	93	5	22	-54	-76	-12	4.43	0.18	35.44	1.44	3	93	5	21	-54	-77	-12	4.82	1.28	38.56	10.24
59	r	Maybush car park, Valley next to river, pw50	3.488	52.052161	1.331662	5	6.5	92	1	15	-85	-112	-15	1.85	1.4	14.80	1.40	3	92	2	15	-81	-112	-21	2.4	0.4	18.70	3.20
62	r	Bucklesham, south beam, behind nearby trees	3.287	52.030018	1.269457	23	8	93	1	10	-87	-116	-16	0.458	0.21	3.66	1.68										0.00	0.00
63	r	Bucklesham, south beam, no near trees	3.265	52.029801	1.272408	23										0.00	0.00										0.00	0.00
64	r	Brightwell, A1093, surrounded by local clutter, then open	2.062	52.040135	1.278876	23										0.00	0.00										0.00	0.00
66	b	Levington, Bridge Rd/Church Ln, surrounded by houses mid village, pv	6.201	52.005856	1.25229	20										0.00	0.00										0.00	0.00
67	b	Levington, Church Lane, just outside village no houses around, pw66	6.295	52.004376	1.255303	9										0.00	0.00										0.00	0.00
68	b	Levington, old A45, no trees on path, pw69	5.683	52.007523	1.278758	25										0.00	0.00										0.00	0.00
69	r	Levington, old A45, pw68	5.059	52.013843	1.268462	28										0.00	0.00										0.00	0.00
71	b/r	Nacton, The Street, mid-village more houses, pw71/73	5.643	52.016899	1.23472	27										0.00	0.00										0.00	0.00
72	r/b	Nacton, Finneys Drift, mid-village a few houses on path, pw72/73	5.513	52.017825	1.235881	25										0.00	0.00										0.00	0.00
73	b/n	Nacton, Levington Rd, out of coverage	6.03	52.013738	1.232216	24										0.00	0.00										0.00	0.00
74	r	Nacton, Ipswich Rd, red coverage surrounded by blue	6.205	52.019234	1.21744	32	8									0.00	0.00										0.00	0.00
75	n/b	Grundisburgh, Stoney Rd, The Dog	6.542	52.112823	1.244584	28										0.00	0.00	3	91								0.00	0.00
76	b	Grundisburgh, Gull Lane, red coverage after blue and null areas, pw10	6.939	52.113602	1.233754	34	8	91	3	21	-71	-100	-23	6.18	1.08	49.44	8.64	3	91	2	18	-75	-105	-23	3.27	0.776	26.16	6.21
77	r	Grundisburgh, Clopton Rd, out of 7km, red after blue, hill after river v	7.793	52.115737	1.215692	51	8	91	4	25	-62	-94	-23	6.13	1.23	49.04	9.84	3	91	2	25	-70	-96	-12	6.02	1.61	48.16	12.88
78	r	Great Bealings, Boot St, mid village, pw81	4.484	52.093078	1.247709	19	8	91	3	20	-71	-101	-22	5.43	1.39	43.44	11.12	3	91	1	16	-82	-105	-12	3.8	0.623	30.40	4.98
79	b/r	Great Bealings, Boot St, out of village	4.248	52.093653	1.257003	21										0.00	0.00										0.00	0.00
80	r	Great Bealings, Holly Lane, out of village	4.472	52.091324	1.243696	33	8	91	2	18	-78	-103	-18	4.43	1.09	35.44	8.72	3	91	1	11	-87	-115	-11	2.8	0.357	22.40	2.86
81	r	Great Bealings, Chapel Lane, behind trees same dir as 78, pw78	5.105	52.097678	1.242522	18										0.00	0.00										0.00	0.00
82	r	Culpho, another far away notspot, village	5.714	52.099256	1.230595	40	8	91	1	9	-89	-115	-12	1.75	0.12	14.00	0.96	3	91	1	8	-86	-116	-22	1.61	0.074	12.88	0.59
83	b/r	Little Bealings, Sandy Lane, Admiral's Head Car Park, pw84, no clutter	3.471	52.084222	1.252721	13	8	91	1	11	-87	-114	-13	2.08	0.238	16.64	1.90	3	91	0	0	-99	-130	-28	0.045	0.007	0.36	0.06
84	r/b	Little Bealings, The Street, pw83, with clutter	3.484	52.084563	1.253189	14	8	91	1	9	-86	-116	-25	1.58	0.109	12.64	0.87										0.00	0.00
85	b/n	Kesgrave Hall, Hall Rd, Milsoms - Lower car park in trees,p86	2.158	52.070653	1.256995	16										0.00	0.00										0.00	0.00
86	r/b	Kesgrave Hall, Hall Rd, Milsoms - Upper car park in trees,p85	2.127	52.069966	1.25671	33	8									0.00	0.00										0.00	0.00

87	b	Heath Lane, urban, surrounded by houses	5.55	52.054199	1.200867	37										0.00	0.00										0.00	0.00
88	b	Ipswich, Colchester Rd, urban, main road	6.328	52.066339	1.190022	44	8									0.00	0.00										0.00	0.00
89	b/n	Melton, Station car park, edge of coverage, check other side rail	6.359	52.1044	1.337454	0										0.00	0.00										0.00	0.00
90	r	Brightwell, Kennels Rd, by A12, main beam behind trees,pw91	2.36	52.040943	1.262576	22	8	93	5	28	-56	-87	-24	5.57	2.25	44.56	18.00	3	93	4	26	-58	-90	-23	4.47	1.92	35.76	15.36
91	r/b	Purdis Farm, Hall Road, out of main beam, pw90	2.467	52.046157	1.251867	14	8	93	1	15	-85	-111	-16	2.3	0.59	18.40	4.72	3	93	1	11	-86	-112	-12	1.99	0.12	15.92	0.96
92	r/b	Woodbridge, Old Barrack Rd, Duke of York car park, suburban	3.308	52.086806	1.297108	34										0.00	0.00										0.00	0.00
93	r/b	Martlesham, Bealings Road, Red Lion car park, close to valley	2.08	52.077226	1.284535	63	no signal									0.00	0.00	no signal									0.00	0.00
94	b	Warren Heath, B&Q car park, industrial estate	5.925	52.032248	1.206424	37	8	93	0	5	-94	-123	-14	1.66	0.065	13.28	0.52										0.00	0.00
95	b/r	Newbourne, The Fox Inn car park, no near trees pw111	3.009	52.039852	1.313452											0.00	0.00										0.00	0.00
96	n/b	Kirton, Innocence Lane, edge of coverage, pw97	6.501	52.003004	1.311122	21	8	93	1	10	-84	-110	-8	1.87	0.67	14.96	5.36										0.00	0.00
97	n	Kirton, Falkenham Rd, out of coverage, 7km,pw96	6.837	52.003536	1.326195	21										0.00	0.00										0.00	0.00
98	b/n	Chelmondiston, Hill Farm Lane, beyond River Orwell,pw99/100	8.837	51.990917	1.214041	27										0.00	0.00										0.00	0.00
99	b	Wolverstone, off Nelson's Ave, beyond River Orwell,pw98/100	9.088	52.000694	1.187985	30										0.00	0.00										0.00	0.00
100	n/b	Freston, Boot cark park, beyond River Orwell,pw99/98	9.42	52.01219	1.166527	30										0.00	0.00										0.00	0.00
101	r/b	Burgh, Burgh Farm, patch of red coverage	7.092	52.121077	1.260874	39	8	91	1	12	-86	-113	-12	1.74	0.703	13.92	5.62	3	91	1	8	-89	-115	-16	1.39	0.064	11.12	0.51
102	r	Swilland, Stoney Rd, Bond's Corner, pw103/104/105, radial	8.064	52.12273	1.226629	41	too many trees									0.00	0.00										0.00	0.00
103	b	Swilland, Charity Lane, Grundisburgh Corner, pw76, pw102/104/105,	8.806	52.128401	1.220834	31										0.00	0.00										0.00	0.00
104	b/n	Swilland, Charity Lane, entrance to Stanaway Farm, pw102/103/105,	9.844	52.136824	1.214237	57	8	91	1	4	-97	-118	-17	2.24	0.453	17.92	3.62										0.00	0.00
105	n	Swilland, B1078, Otley College, pw102/103/104, radial, out of coverag	10.363	52.141588	1.212675	59	8	91	1	3	-100	-123	-21	1.84	0.353	14.72	2.82										0.00	0.00
106	r	Outside Adastral, trees, pw107	0.595	52.060954	1.289552											0.00	0.00										0.00	0.00
107	r	Outside Adastral, trees, pw106	0.598	52.059961	1.290187											0.00	0.00	3	91								0.00	0.00
108	b/n	Sutton, Melton Road, open, 7km distance, on hill, pw9, in coverage	6.62	52.086984	1.366869											0.00	0.00										0.00	0.00
109	r	Brightwell, Ipswich Road, pw18, no immediate clutter	1.006	52.050348	1.287777	not done because there is no area without trees										0.00	0.00										0.00	0.00
110	r	Martlesham, no trees, pw39	1.399	52.070414	1.274678	32	8	91	3	22	-70	-93	-9	4.72	1.31	37.76	10.48	3	91	3	19	-77	-94	-8	3.7	1.14	29.60	9.12
111	b	Newbourne, behind quite a lot of trees, pw95	3.033	52.04095	1.31554											0.00	0.00										0.00	0.00

Annex C: Consultancy on Using LTE to Control Robots in Oil Refinery

The study below is part of a technical consultation realized for BT Global Services on behalf of a known petrol extraction company (Shell).

Shell's core business is the exploration, refining and distribution of oil and gas products. As the oil and gas production is moving to more hazardous environments, Shell started to develop Sensabot, a compact battery powered machine designed to remotely inspect hazardous industrial facilities. This machine is operated by remote control and equipped with 10 video cameras, a laser scanner and a number of environmental sensors to detect poisonous gasses. Sensabot will enable Shell to reduce worker exposure in remote, unmanned hazardous facilities; enable safer operations; and enable more efficient operations.

In order to make Sensabot a reality a system to control it wirelessly needs to be deployed. One of the technologies considered was LTE. These robots require between 20-30 Mbps upload capacity and low latency, at the same time Shell didn't want a proprietary solution with proprietary hardware, so a standard based solution was preferred. From previous work on wireless networks, it was decided LTE TDD would be more adequate in this case, because of its capability to control the amount of spectrum used for upload/download (as the upload capacity was much higher than the download). LTE allows for bigger amounts of spectrum to be used and it was the technology which was being embraced around the world (see Figure 13 in Section 3.4.2). Shell technical consultants were also provided with a tutorial on LTE transmissions and architecture by the author and this technology was agreed.

Another constraint on the overall design was that the number of robots per site would be very small 10-15 and therefore an expensive full size mobile operator core network was to be avoided. For this, several manufacturers were found that could provide virtualized or single box EPC solutions, ranging from half a rack to 2 units size (a medium size basic mobile operator would require a minimum 5-8 racks of equipment for the core, without taking redundancy into account).

After getting in contact with several LTE equipment vendors, Huawei was selected as the partner to trial the technology. The tests were performed under lab conditions and in an urban environment at the Huawei test facilities in Shanghai. These PoC tests were aimed to establish what could be achieved with LTE wireless technology available today, the tests were based upon a single Sensabot, but that was sufficient to demonstrate the capabilities and limitations of the technology.

With the joint efforts of Huawei and BT Global Services the PoC designed for the Shell Sensabot project demonstrated how an LTE system can be adapted to deliver the requisites for Sensabot deployment, especially the high uplink speeds required for a single Sensabot

(10HD video streams, approx. 42 Mbps), and the low latency (<100ms one way, <500ms roundtrip) essential for smooth Sensabot operation. The tests run for 2 days delivering results for the 32 test cases including both lab test (Figure 113) and field test (Figure 114). The highlights from these tests were:

- As mentioned in the above section, a single test UE was able to provide more than 42 Mbps throughput for the uplink both in cell center and cell middle (up to 60 Mbps). Huawei's commercial single LTE cell's capacity and coverage capability could fulfill the huge uplink bandwidth consumption generated by 10 full HD cameras per robot.
- The latency was noticeably low in all the test area (lower than 30ms) because the network was not being used by anyone else, which is a good reflection of the deployment scenario. This feature is crucial for the real time control of Sensabot. Even when handovers happened, the latency was still less than 30ms.
- The handover procedure was carefully tested. In the field test, during handover, the uplink UDP throughput decreased to 37.8 Mbps from a maximum of 60 Mbps, but the downlink connection remained solid. That means that even during handover, we would still be able to obtain solid control over the robots.

While the radio environment tests were performed, Huawei also demonstrated their small core equipment in a real environment. This small core equipment is key for private deployments, in terms of bandwidth needed (much less than a mobile operator), CAPEX and OPEX. For comparison a typical core network would require at least 5-8 cabinets, while Huawei's small core solution would fit in a single half frame.

Summary

During the test process and workshop conversations in Shanghai, it was concluded that the current Huawei LTE infrastructure provided sufficient support for the Sensabot application.

There are still several issues that need to be taken into account to assure the best throughput and coverage performance that can only be designed on each of the actual locations of deployment via careful radio planning taking into account the local environment (e.g. use of high gain antennas, careful planning to minimize interference, but maximize middle cell coverage avoiding cell edge, the type of antenna used in the UE, integration with Wi-Fi to increase the bandwidth). For example, in a normal coverage area, the peak performance between 5dBi and 2dBi is similar, but more noticeable dips are observed when using 2dBi antenna which means that 2dBi antenna is more likely to be influenced by environmental factor than 5dBi one. In weak coverage area, the throughput of 2dBi antenna is noticeable lower than 5dBi antenna.

To summarize, the PoC test in Shanghai demonstrated the readiness of LTE TDD technology to cover the needs of Shell.

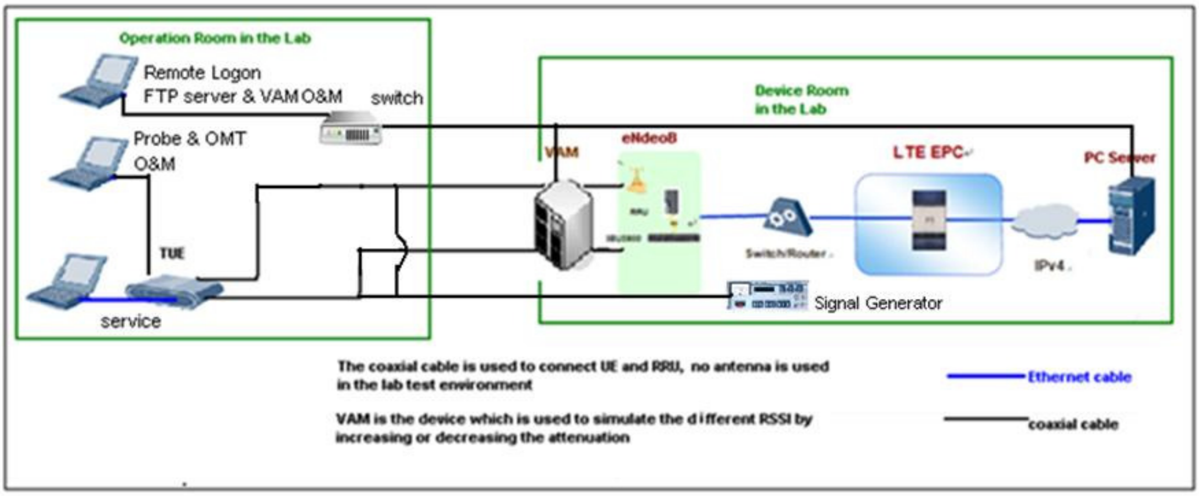


Figure 113 - Lab environment (Source: Huawei Labs).

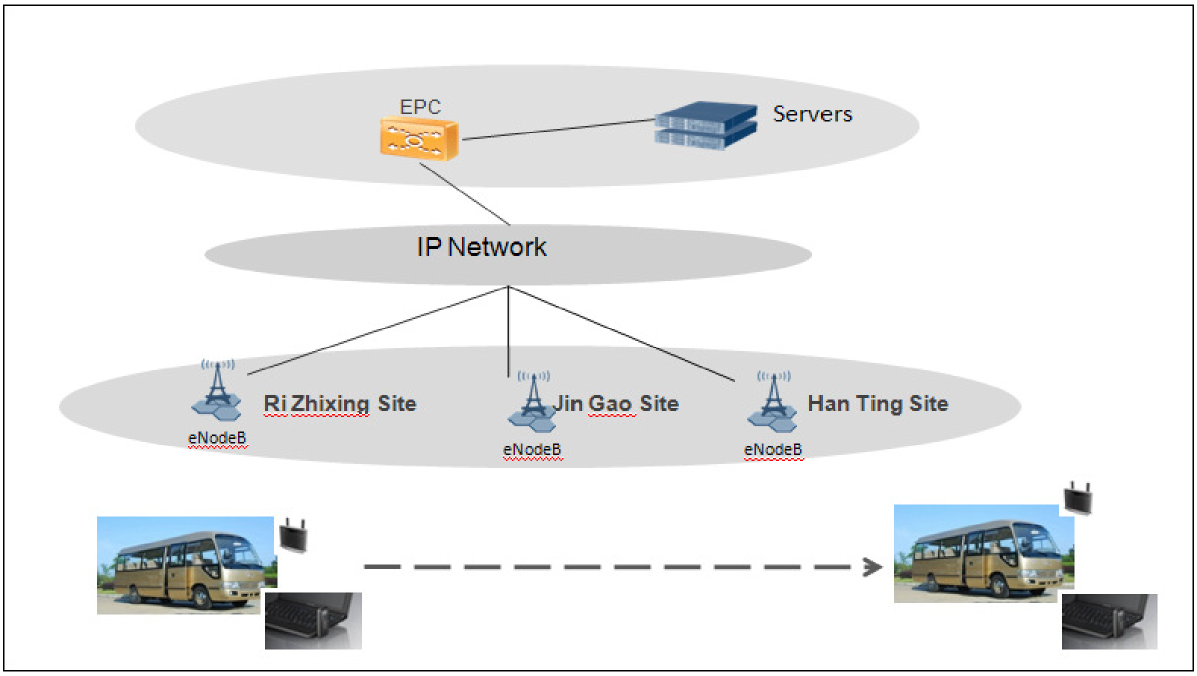


Figure 114 - Field test scenario (Source: Huawei Labs).

Annex D: On Board Wi-Fi Trialist Briefing and Test Description

Volunteer Testing Brief

What We Plan to Do:

- We are looking to test the behaviour of the Wi-Fi service provided inside an EasyJet plane
- The test will be conducted in segments and we'll be asking you for feedback at key intervals via the 'Test Feedback' sheet

What We Need from You:

- We need your help to perform wireless testing using your smartphone device(s), tablets and laptops. Please bring any wifi devices you would like to use while in flight.
- We need you to be patient as this is a repetitive activity (but will really help us to stress-test a new EasyJet capability)
- We ask you to provide a 'score' for how you feel the Wi-Fi service performed, from extremely poor (1) to extremely good (10)

How We Need You to Do it:

- **Please ensure you enter the plane with your device in flight-mode.**
- You will each be directed to a seat in the plane. Please note the seat number as it will tell us your location within the plane
- We will ask you to connect to the Wi-Fi service (not 3G) using the SSID **BT-EasyWifi** via your normal method and check connectivity is working. Please ensure that all your devices are in flight mode, and turn on Wifi only when told (please disable Bluetooth, GPS and 3G/2G). **Make sure you know how to turn on wifi only and how to connect to a specific Wifi access point**
  - If there are any problems getting online with BT-EasyWifi, please raise your hand.
- Once connected we want you to perform a number of activities (please wait for directions), ranging from your normal web browsing and applications (BT, eBay, etc) reading news (BBC, Sky, MSN, etc), updating social networks (Facebook, Twitter, etc) but please DO NOT conduct streaming activity (ie. no videos, iplayer, youtube) unless specifically asked to by the group lead

How We Are Structured:

- We have a simple structure of 2 teams. Team leaders will communicate the timings of when to capture your scores and when to answer questions, they may also give you specific individual instructions (e.g. please start streaming from You-Tube)

Services to Use When Asked:

- Web: bbc.co.uk, easyjet.co.uk, thetimes.co.uk, youtube.com, content address, Sky, Sky Sports, The Sun, MSN, London2012.com, Google, Yahoo, Wikipedia. TFL.gov.uk, trainline.com, BT, Spotify, Wimbledon
- Shopping: Amazon, eBay, Tesco, DABS
- Social sites: Bebo, Twitter, Facebook
- Video sites: YouTube, iPlayer, skyplayer

Pre-tasks for Trialist on Easyjet

Task 1: Verify Device Movie Player Can Use Content Server

1. Please verify that your device can play the video in the following website:
2. http://nat.cdndvlab.bt.co.uk/smartplayer/demo.html
3. If your device browser can play this file, this is a good device to take to the trial.
4. If you can't play this file, if using a laptop update your browser or try downloading Google Chrome latest version; if you are using a IOS device, try other browsers if available from App Store; if an Android device try downloading Google Chrome browser or dolphin browser from the google play store and try to play the above video again.

Task 2: Find the Wifi MAC Address of the Device

For Android Devices:

1. Under your Applications, select **Settings**
2. At the very bottom of the list, choose "**About Device** (Android Phones may say **About Phone**)
3. Choose **Hardware Information/Status**
4. Your MAC address will be listed under Wi-Fi MAC Address.

For IOs Devices:

1. Tap Settings
2. Select General.
3. Select About.
4. The Mac address is listed as Wi-Fi Address.

For RIM Devices:

BlackBerry Device Software 4.5 to 5.0:

1. From the **Home Screen** click on **Options.**
2. Next click **Status.**
3. The **WLAN MAC** field displays the MAC address for the BlackBerry smartphone.

BlackBerry Device Software 6.0 to 7.1:

1. From the **Home Screen** select **Setup.**
2. Next select **Options.**
3. Next select **Device.**
4. Then select **Device and Status Information.**
5. The **WLAN MAC** field displays the MAC address for the BlackBerry smartphone.

For Windows XP/Vista/7

1. Click on **Start**
2. Click on **run** or **search** and write **cmd** press enter
3. Type the following command: **ipconfig /all**

4. Search for your wireless **"Wireless LAN adapter Wireless Network Connection"** and get the **"Physical address"** field.

For Windows 8

1. Press **Windows Key + C** to open Windows Charms bar and click on Search. In the Search field type **cmd**.

2. The result comes. Right-click on it and click on **Run as Administrator**. If prompted by UAC, click Yes to continue.

3. Type the following command
ipconfig –all

4. Search for your wireless **"Wireless LAN adapter Wireless Network Connection"** and get the **"Physical address"** field.

For Macs:

1. Open System Preferences from the Apple menu
2. Click on "Network"
3. Select your currently active network connection from the left menu (Wi-Fi, Ethernet, etc) and then click on "Advanced" in the lower right corner
4. Look at the bottom of the window for "Wi-Fi Address", the hexadecimal characters next to this are the machines MAC address

Task 3: Download Speedtest App for Android and IOs

For IOS and Android devices only, download the speedtest.net:

http://www.speedtest.net/mobile.php.

Also try http://www.mybroadbandspeed.co.uk/ and run a speedtest from there.

Task 4: Bookmark the Following Addresses

In order to limit the time wasted typing web address please bookmark the following websites:

http://bt-easywifi.com

http://bt-easywifi.com:5080

http://bt-easycache.com/mirror

http://bt-easycache.com/mirror/speedtest

http://bbc.co.uk/news

http://www.mybroadbandspeed.co.uk/

www.thetimes.co.uk

www.guardian.co.uk

Task 5: Please Remember to Bring a Pen to the Plane!

Volunteer Testing Pack

The volunteers were divided in two teams (team 1 and team 2) to run different tasks at the same time. The below briefs were given on the day.

Volunteer Test Briefing – Team 1

Please have your device off before entering the plane and starting tests. Seat in any seat in the left side of the plane try to make it an even distribution so if you see an area very empty go and sit there. Please record the seat number you are using in the Volunteer feedback form. When told to, please:

- **Test 1:** Switch on device, switch on wifi. **Disable 3G if applicable**. Connect to the EasyWifi Wifi Access point, make sure your **3G data is off.** Go to landing website manually and wait for further instructions:
  - http://easywifi.com
  - Please annotate any feedback in test sheet (keep providing feedback subsequent tests)
- **Test 2:** Click on the Easyjet banner and make the normal actions to book a ticket. Free use within the Easyjet site for 5min.
- **Test 3:** Download a file from the website below in the Speed test area (5min). Please tell us in the feedback sheet how was your perception of the download, note it is 116MB (as expected, faster than expected, slower than expected…)
  - http://easywifi.com/ (this can change as not yet defined)
  - **Test 4:** Go back to the landing page (http://easywifi.com)Click on the wifi content banner and start watching one of the videos. Free use of this website for 5min
- **Test 5:** Connect to www.BBC.co.uk/news and browse within the site without streaming videos for 5min (BBC is pre-cached at 7 levels)

- **Test 6:** Connect to www.thetimes.co.uk. And browse it for 5min (The Times is not pre-cached but will be cached progressively as users access). Please provide comparison of experience with bbc.co.uk/news in test sheet notes
- **Test 7:** Stress wifi. Everyone team 1 &2 connects to content website to watch videos for 2 min
  - Content: http://easycache.com/mirror/
- **Test 8:** Free internet/app usage, except voip and video streaming for 5min
- **Test 9:** Free internet/app usage including voip and video streaming for 5min
- **Test 10:** Everyone is allowed to access any service they wish to for 5-10min
- **Test 11:** complete online survey on:
  - www.forwizee..... (Daniel to provide address)

Volunteer Test Briefing – Team 2

Please have your device off before entering the plane and starting tests. Seat in any seat on the right of the plane try to make it an even distribution so if you see an area very empty go and sit there. Please record the seat number you are using in the Volunteer feedback form. When told to, please:

- **Test 1:** Switch on device, switch on wifi. **Disable 3G if applicable**. Connect to the EasyWifi Wifi Access point, make sure your **3G data is off.** Go to landing website manually and wait for further instructions:
  - http://easywifi.com
  - Please annotate any feedback in test sheet (keep providing feedback subsequent tests)
- **Test 2:** Click on the wifi content banner and start watching one of the videos. Free use of this website for 5min.
- **Test 3:** Download a file from the website below in the Speed test area (5min). Please tell us in the feedback sheet how was your perception of the download, note it is 116MB (as expected, faster than expected, slower than expected…)
  - http://easywifi.com/ (this can change as not yet defined)
  - **Test 4:** Speed tests, please annotate speeds and delay. 2min (repeat 2-3 times)
  - 4a:**If you have a laptop** go to http://www.mybroadbandspeed.co.uk/ (live internet)
  - 4a:**If you have an IOs device or Android** use speedtest.net app that we asked you to preload in the testing brief.
  - 4b: Users with **laptops or devices with flash capability** (laptops, macs, high-end androids), after doing task 4a please go to http://easycache.com/mirror/speedtest and annotate the download speed. 2min
- **Test 5:** Connect to www.BBC.co.uk/news and browse within the site without streaming videos for 5min (BBC is pre-cached at 7 levels)

- **Test 6:** 1 Connect www.guardian.co.uk and browse it for 5min (The Guardian will not be cached). Please provide comparison of experience with bbc.co.uk/news.
- **Test 7:** Stress wifi. Everyone team 1 &2 connects to content website to watch videos.
  - Content: http://easycache.com/mirror/
- **Test 8:** continue watching videos
- **Test 9:** continue watching videos
- **Test 10:** Free usage of the internet including streaming and VoIP for 5-10min
- **Test 11:** complete online survey on:
  - www.forwizee..... (Daniel to provide)

Volunteer Test Feedback Form– Team 1

Volunteer Test Feedback – Team 1

Name:	e-mail:
Device(s):	Device(s) Wi-Fi MAC:
Seat number:	

Please grade the level of service you received whilst testing between 1 and 10.

1____________________________________10

extremely poor extremely good

If you were unable to test at the time a score is requested please use 'none' and explain issue.

Test	Score 1-10	Did your connection drop out?	Comments Any device problems (hangs, crashes, drops) & what sites\streaming tools used?
Test 1			
Test 2			
Test 3			
Test 4			
Test 5			
Test 6			
Test 7			
Test 8			
Test 9			
Test 10			

Wi-Fi testing 19/03/13

Volunteer Test Feedback Form– Team 2

Volunteer Test Feedback – Team 2

Name: e-mail:
Device(s): Device(s) Wi-Fi MAC:
Seat number:

Please grade the level of service you received whilst testing between 1 and 10.

1____________________________________10

extremely poor extremely good

If you were unable to test at the time a score is requested please use 'none' and explain issue.

Test	Score 1-10	Did your connection drop out?	Comments Any device problems (hangs, crashes, drops) & what sites\streaming tools used?
Test 1			
Test 2			
Test 3			
Test 4 4a			
4b			
Test 5			
Test 6			
Test 7			
Test 8			
Test 9			
Test 10			

Wi-Fi testing 19/03/13